appviewx

CERT+ Guides

Version: 2024.3.0.0

Copyright AppViewX, Inc.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface 19

Revision History 19

About this Guide 19

Audience 19

Third-Party Software Acknowledgments 19

Text Conventions 19

Chapter 1. Getting Started 21

Know your Deployments for CERT+ 21

Key Capabilities of CERT+ 22

Discovery and Visibility 22

Inventory and Management 22

Dashboard for Visibility and Monitoring 22

CLM Automation 23

Cloud and DevOps 23

Secure Key Management 23

Certificate and Key Compliance 23

IoT and Enterprise Mobility Certificate Management 24

SSH Key Lifecycle Automation 24

Alerts & Logs 24

Groups & Policies 24

Administration 25

Start with Your Onboarding Journey 25

Subscribe AppViewX Trial Application 26

Onboarding Journey 28

Remediate Certificate Issues 39

CERT+ Requirement and Access 45

RBAC Configuration 48

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Benefits of RBAC....48
Simplified RBAC Configuration in AppViewX....49
Enabling RBAC for CERT+ Native Workflows....49
Invite Teammates to Your AppViewX Trial....51
Chapter 2. CERT+ User Guide....52
Onboarding Certificates....52
Prerequisites for Onboarding Certificates....53
Certificate Discovery....53
Discovery Status....129
Discovery Exclusions....140
Discovery Configuration....141
Syncing Certificates with Network Devices or Servers....157
Manage Devices....159
Inventory Actions....159
Device Prerequisite....165
ADC Prerequisite....165
Firewall and Web Application Firewall (WAF) Prerequisite....171
Prerequisites for Cloudflare - AppViewX CLM....174
Server Prerequisite....179
Certificate Actions....183
Enrolling Certificates....184
Renewing Certificates....257
Pushing Certificates to Devices....266
Reissuing Certificates....462
Revoking Certificates....465
Regenerating Certificates....473
Reinstating Certificates....479
Duplicating Certificates....481
Running Revocation Check-OCSP....483

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Generating Certificate Signing Request (CSR)..... 486
Migrating CAs (CA Switch)..... 491
Running the SSL Checker for a Certificate..... 503
Managing the Certificate Inventory..... 503
Managing the Server Certificate Inventory..... 504
Managing the Client Certificate Inventory..... 515
Managing the Code Signing Certificate Inventory..... 525
Managing the Device Certificate Inventory..... 533
Managing the Intermediate Certificate Inventory..... 540
Managing the Root Certificate Inventory..... 541
Uploading a Certificate..... 542
Downloading Certificates..... 543
Archiving Certificates..... 550
Certificate Reporting and Monitoring..... 557
Accessing the Dashboard..... 558
Creating a Dashboard..... 559
Exporting Dashboard Information..... 560
Importing a Dashboard..... 560
Understanding Certificate Reports on the Dashboard..... 561
Searching for Dashboard, Object, or Widget..... 613
Deleting a Dashboard..... 613
Insights..... 613
Accessing the Discovery Summary Dashboard..... 658
Alerts and Logs..... 665
Overview..... 665
Certificate Alerts..... 665
Configuring Expiry Alerts..... 666
Configuring a Certificate Expiry Alert 692
Configuring a Certificate Sync Alert 693

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a Certificate Validation Alert 695
Configuring a Connection Failure Alert 696
Configuring a CLM Action Failure Alert 697
Certificate Logs 700
Export Certificates Logs 701
Managing Certificates Using Automation Workflows 702
Getting Started 702
Certificate Expiry Workflows 706
Certificate Enrollment Workflows 725
Renew Certificate Workflows 796
Automation Workflow Tasks 825
Designing a Custom Workflow using OOB Tasks 876
Scheduling an OOB workflow 883
Customizing an OOB Workflow 883
Managing Certificates Using AppViewX Terraform Provider 884
What is Terraform? 884
How does Terraform work? 885
What AppViewX Terraform Provider does? 886
Where is AppViewX Terraform Provider Hosted? 886
Supported Authentication Models 887
Supported APIs and Details 887
How to use AppViewX Terraform Provider? 887
Sample Provider and Resources .tf files 897
Troubleshooting 900
Enhancements Implemented 901
Use Cases supported in AppViewX Terraform Registry v1.0.1 901
Future Roadmap Items 901
Points to Remember 902
Standard Practices 902

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

PKI Standard Practices....902
CLM - Best Practices....905
Standard Practices followed in the Certificate Inventory Management 906
Securing CERT+....908
Chapter 3. CERT+ Admin Guide....909
Configuring CA Settings....910
Amazon and Amazon Private CA....911
CSC Global CA....932
Custom CA....936
DigiCert CA....939
DigiCert MPKI 943
DigiCert One....946
EJBCA 950
Entrust CA....953
Entrust MPKI....956
Futurex....959
GlobalSign MSSL CA....963
GlobalSign Atlas CA....967
GlobalSign SSL CA....971
GoDaddy CA....974
Google CA....978
HashiCorp Vault CA....981
HydrantID CA....986
IDnomic CA....989
InCommon CA....994
Let’s Encrypt CA....998
Microsoft Enterprise CA....1000
Microsoft Standalone CA....1008
Nexus CA....1015

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sectigo CA....1018
SwissSign CA....1024
Symantec CA....1028
Trustwave CA....1030
CA Policy....1033
Configuring Policy Details....1035
Configuring a CA Policy for Amazon CA....1036
Configuring a CA Policy for Amazon Private CA....1039
Configuring a CA Policy for Digicert CA....1043
Configuring a CA Policy for Digicert One CA....1047
Configuring a CA Policy for EJBCA CA....1052
Configuring a CA Policy for Entrust CA....1055
Configuring a CA Policy for Entrust MPKI CA....1060
Configuring a CA Policy for Futurex....1063
Configuring a CA Policy for GlobalSign Atlas CA....1069
Configuring a CA Policy for GlobalSign CA....1073
Configuring a CA Policy for GlobalSign MSSL CA....1077
Configuring a CA Policy for GoDaddy CA....1081
Configuring a CA Policy for Google CA....1085
Configuring a CA Policy for HashiCorp Vault CA....1090
Configuring a CA Policy for HydrantID CA....1094
Configuring a CA Policy for IDnomic CA....1098
Configuring a CA Policy for Let's Encrypt CA....1102
Configuring a CA Policy for Microsoft Enterprise CA....1106
Configuring a CA Policy for Microsoft Standalone CA....1110
Configuring a CA Policy for Nexus CA....1114
Configuring a CA Policy for OpenTrust CA....1118
Configuring a CA Policy for Sectigo CA....1122
Configuring a CA Policy for Symantec CA....1126

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a CA Policy for Trustwave CA..... 1130
Configuring Certificate Groups.....1134
Configuring Certificates.....1143
Configuring Certificate Settings..... 1143
Configuring Certificate Attributes..... 1145
Configuring Certificate Profiles..... 1148
Managing Certificate History.....1151
Managing Expired Certificates.....1154
Configuring and Managing Devices.....1155
Configuring ADC Devices..... 1155
Configuring and Managing Servers 1196
Configuring and Managing Firewalls 1428
Configuring Switches..... 1464
Configuring Routers..... 1466
Configuring and Managing Cloud Devices..... 1469
Configuring WAFs.....1592
Certificate Reports..... 1613
Auto-Enrollment Protocols.....1621
EST..... 1622
ACME..... 1723
SCEP 1864
MS Intune.....1893
CMP..... 1925
WAEP.....1948
Actions 2011
Direct Requests..... 2012
MDM Device Integration for Certificate Lifecycle Management.....2014
AppViewX Integration with JAMF..... 2015
Configuring General Settings.....2032

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Appendix A: Prerequisites for Enabling the Integrated Windows Gateway Mode..... 2035
Appendix B: List of Scheduled Jobs.....2044
..... 2044
Auto Regenerate Certificates.....2044
Automated Credential Rotation.....2045
Auto-Renew Certificates..... 2045
CA Connector Validity Updater.....2045
Certificate CAA Record Check..... 2045
Certificate Compliance Check..... 2046
Certificate Expiry Status Check..... 2047
Certificate Polling Request..... 2047
Certificate Revoke Status Check From CA..... 2047
Certificate Transparency Check..... 2047
Certificate Validation Check.....2048
Certificate Vulnerability Check..... 2049
CRL Certificate Revocation Check..... 2050
CRL Download Monitor Job.....2050
Delete Expired Certificates..... 2050
Device and Certificate synchronization..... 2051
Periodic CRL Update for AppViewX and Custom CAs..... 2051
Working with the Job Scheduler..... 2052
Chapter 4. CERT+ API Guide..... 2055
API Reference..... 2055
Enable ACF Permission for API Reference..... 2055
Best Practices for Working with the AppViewX API..... 2056
Understanding the AppViewX CERT+ API..... 2056
RESTful HTTPS Requests..... 2056
Requests..... 2057
Request Structure..... 2058

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure..... 2058
Description of Server Responses..... 2059
URI Scheme..... 2059
Types of Accounts in AppViewX..... 2059
Authentication using a User Account..... 2060
Retrieve session ID using login API..... 2060
Using Session ID for further API calls..... 2064
Authentication using a Service Account..... 2070
Retrieve Access Token using get-service-token API..... 2071
Using Access Token in the header for further API calls..... 2074
CLM API..... 2078
Create a Certificate in Async mode..... 2080
Create a Certificate in Sync mode..... 2205
Renew a Certificate in Async mode..... 2219
Renew a Certificate in Sync mode..... 2226
Revoke a Certificate in Async mode..... 2236
Revoke a Certificate in Sync mode..... 2243
Reissue a Certificate in Async mode..... 2248
Reissue a Certificate in Sync mode..... 2256
Regenerate a Certificate in Async mode..... 2267
Regenerate a Certificate in Sync mode..... 2274
Suspend a Certificate..... 2282
Reinstate a Certificate..... 2289
Search/Get Certificate Inventory..... 2295
Add Certificate Attributes..... 2307
Add Multiple Certificate Attributes..... 2314
Update Certificate Attributes..... 2320
Get Certificate Attributes..... 2326
Delete Certificate Attributes..... 2330

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Delete Multiple Certificate Attributes..... 2334
Bulk Add/Update Certificate Attributes..... 2340
Fetch List of Server Devices..... 2347
Download a Certificate.....2354
Download a Certificate by Format..... 2359
Download Private Key of a Certificate.....2365
Common Response Objects.....2371
Push and Bind Certificate to a Firewall Profile.....2372
Rollback Certificate to Firewall Profile.....2382
Get Available Server Profiles.....2387
Push and Bind Certificate to a Server Profile..... 2393
Rollback Certificate to Server Profile.....2421
Delete Certificate using UUID.....2427
Discover Certificates from Firewall..... 2431
Discover Certificates from Server.....2438
Discover Certificates from CT Log..... 2445
Discover Certificates from Network..... 2479
Network Discovery Configuration..... 2618
Fetch Single Certificate Discovery.....2648
Fetch Certificate Discovery Results by Discovery Name..... 2656
Fetch Devices Discovered During a Network Scan..... 2677
Fetch Cipher–TLS Version Mapping from Discovery Execution.....2682
Delete Certificate Discovery..... 2691
Upload Multiple Certificates to the Inventory.....2694
Upload Server Certificate to the Inventory..... 2702
View a Certificate Group..... 2707
Create a Certificate Group..... 2714
Update a Certificate Group.....2722
Delete a Certificate Group.....2731

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Assigning ACL Permissions for Resources....2735
Trigger Profile Sync for Devices....2742
List Certificates with Application Connector Details....2749
List Certificate Groups....2768
Use Insights to Create a Centralized CERT+ Dashboard....2778
Assign Certificates to a Group....2798
Unassign Certificates from a Group....2805
Archive Certificates....2813
Recover Archived Certificates....2818
ADC+ API (for CERT+)....2823
Push and Bind Certificate to ADC Devices....2824
Push and Bind Certificate to ADC Profile....2851
Rollback Certificate to ADC profile....2874
MultiCloud API....2880
Push Certificates to ACM....2881
Push Certificates to IAM....2890
Push Certificates to ELB via ACM....2899
Push Certificates to ELB via IAM....2909
Push Certificates to Cloudfront via ACM....2918
Push Certificates to Cloudfront via IAM....2928
Push Certificates to Azure Key Vault (Certificate Location)....2938
Push Certificates to Azure Key Vault (Secrets Location)....2947
Push Certificates to Azure Application Gateway (Gateway Listener Profile | Direct upload to Application Gateway)....2957
Push Certificates to Azure Application Gateway (Gateway Listener Profile | Choose from Key Vault)....2966
Push Certificates to Azure Application Gateway (Gateway SSL Profile)....2976
Push Certificates to Azure App Service....2985
Push Certificates to Azure Enterprise Application Service....2995

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Push Certificates to Azure App Registration Service....3004
Push Certificates to Azure API Management Service....3012
Push Certificates to GCP Certificate Manager Service (Scope: Global)....3021
Push Certificates to GCP Certificate Manager Service (Scope: Regional)....3030
Push Certificates to GCP Classic Certificates Service (Scope: Global)....3039
Push Certificates to GCP Classic Certificates Service (Scope: Regional)....3047
Push Certificates to GCP Load Balancer Service (via Classic Certificates)....3056
Push Certificates to GCP Load Balancer Service (via Certificate Manager-Global External LB)....3065
Push Certificates to GCP Load Balancer Service (via Certificate Manager-Regional Internal LB)....3075
Automation Workflows API....3084
Enroll Certificate and Download....3085
Easy Certificate Provisioning....3096
Enroll Certificate and Push....3104
Enroll Certificate with ServiceNow....3119
Enroll Certificate and Push with ServiceNow Integration....3132
Renew Certificate and Push....3144
Renew Certificate with ServiceNow Integration....3156
Renew Certificate and Push With ServiceNow Integration....3168
Regenerate Certificate - With New CSR....3179
Get Request Summary/Log....3192
After you are done....3197
Approve a Request....3197
Implement a Request....3202
Chapter 5. CERT+ Troubleshooting Guide....3208
Troubleshooting for CAs....3208
Troubleshooting for Amazon CA Issues....3208
Troubleshooting for Custom CA Issues....3214

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting for DigiCert CA Issues....3218
Troubleshooting for EJBCA CA Issues....3222
Troubleshooting for Entrust MPKI Issues....3232
Troubleshooting for GlobalSign CA Issues....3235
Troubleshooting for GoDaddy CA Issues....3239
Troubleshooting for Google Private CA Issues....3249
Troubleshooting for InCommon CA Issues....3256
Troubleshooting for LetsEncrypt CA Issues....3265
Troubleshooting for Microsoft Enterprise CA Issues....3269
Troubleshooting for Microsoft Standalone CA Issues....3297
Troubleshooting Sectigo CA....3320
Troubleshooting Symantec CA....3330
Troubleshooting Trustwave CA....3333
Troubleshooting the Windows Agent Setup....3338
Troubleshooting General....3353
Troubleshooting Certificate Group....3353
Troubleshooting Certificate Policy....3355
Troubleshooting Certificate Reports Configuration....3357
Troubleshooting Configuration of Workflow....3358
Troubleshooting Truststore Bundle Deployment....3359
Troubleshooting Auto-Enrolment Protocols....3360
Troubleshooting for ACME....3361
Troubleshooting for EST....3366
Troubleshooting for MsIntune SCEP....3373
Troubleshooting for SCEP....3376
Troubleshooting AWS, CLOUD....3379
Troubleshooting for AWS ACM....3380
Troubleshooting for AWS IAM....3383
Troubleshooting AWS CloudFront....3387

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting AWS ELB 3390
Troubleshooting Azure Cloud 3393
Troubleshooting Cloud - Common Functionality 3402
Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors 3405
Troubleshooting Apache Linux 3406
Troubleshooting Barracuda WAF 3411
Troubleshooting Cisco ASA Firewall 3412
Troubleshooting Cisco CallManager 3413
Troubleshooting Common Functionality of Servers 3415
Troubleshooting Data Power Server 3417
Troubleshooting F5 WAF 3420
Troubleshooting Fortigate Firewall 3424
Troubleshooting HP ILO 3427
Troubleshooting IBMClient Linux 3429
Troubleshooting IBMClient Windows 3431
Troubleshooting Imperva WAF 3434
Troubleshooting Linux JBoss Server 3436
Troubleshooting for Microsoft Enterprise CA Issues 3443
Troubleshooting Microsoft Tomcat 3471
Troubleshooting MQServer Linux 3476
Troubleshooting MQServer Windows 3479
Troubleshooting MS SQL Windows 3481
Troubleshooting Nginx Server 3483
Troubleshooting NginxPlus ADC 3485
Troubleshooting Paloalto Firewall 3487
Troubleshooting Panorama Firewall 3489
Troubleshooting Check point Firewall 3492
Troubleshooting RabbitMQ Server 3493
Troubleshooting Rapid SB Server Inventory 3498

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Rapid SB Linux Server 3501
Troubleshooting Tomcat Linux 3508
Troubleshooting Weblogic Linux 3512
Troubleshooting Websphere Linux 3518
Troubleshooting Websphere Windows 3524
Troubleshooting Windows Apache Server 3526
Troubleshooting Windows JBoss Server 3528
Troubleshooting Windows Weblogic Server 3534
Chapter 6. Key Use Cases 3536
Automating CLM for Akamai CPS 3536
Automating CLM for Apache (Linux) 3559
Automating CLM for Apache (Windows) 3610
Automating CLM for Tomcat (Linux) 3658
Automating CLM for Tomcat (Windows) 3709
Automating CLM for JBoss 3762
Automating CLM for Linux 3822
Automating CLM for Windows Environment 3872
Automating CLM for Microsoft IIS 3942
Automating CLM for Firewall 3992
Automating CLM for Palo Alto 4055
Automating CLM for CheckPoint 4103
Automating CLM for F5 Devices 4148
Automating CLM for Citrix Devices 4222
Automating CLM for AWS Resources 4277
With ACM Integration 4277
With IAM Integration 4386
With ELB Integration 4485
With CloudFront Integration 4587
With EC2 Integration 4687

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Automating CLM for Microsoft Azure Resources..... 4791
With Key Vault Integration.....4791
With Application Gateway Integration.....4860
With Virtual Machines Integration.....4928
With App Service Integration.....5008
With Enterprise Application Integration..... 5076
With API Management Integration.....5146
With App Registration Integration.....5214
With Front Door Integration.....5280
Automating CLM for Microsoft SQL.....5348
AppViewX Integration with MDM devices.....5396
Chapter 7. Glossary.....5414

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Preface

Revision History

Revision	Description	Date
1.0	Initial draft of document for the release v2024.3.0.0	September 2025

About this Guide

This guide provides you step-by-step instructions for performing Certificate Lifecycle Management (Discovery, Monitor, Enroll, Renew, Push, Regenerate, Reissue, Revoke, and Inventorize certificate) and manage organization PKI posture. CERT+ helps you to enroll and manage public and private certificates.

Audience

This guide is intended for everyone deploying AppViewX CERT+ for managing their certificates.

Third-Party Software Acknowledgments

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

For example,

• This document includes software details developed by VMware, Inc. (www.vmware.com).

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Convention	Description
	Vendor/Version/Value is available only for the **on-premise** deployment
	Vendor/Version/Value is available only for the **SaaS** deployment

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 1: Getting Started

Know your Deployments for CERT+

We support multiple deployment options to cater to various customer needs and infrastructure preferences. Our solutions can be deployed in On-Premises environments, Managed Kubernetes platforms such as EKS, AKS,GKE and OpenShift and as a Software as a Service (SaaS).

SaaS Deployment (Highly Secure and Hassle-Free)

Our Software as a Service (SaaS) offering is designed for organizations that prioritize security, simplicity, and efficiency. In this deployment mode, we manage all aspects of application hosting, maintenance, and scaling, providing a worry-free experience for our customers. Our SaaS platform is built with cutting-edge security measures, including robust encryption, multi-factor authentication, and continuous monitoring to ensure your data and operations are protected at all times.

Choosing SaaS not only reduces the burden on your IT teams but also ensures that you benefit from the latest updates, features, and security enhancements without any additional effort. This option is ideal for organizations of all sizes, particularly those looking to quickly access our services with the assurance of enterprise-grade security and compliance. For additional information about saas deployment, click here.

On-Premises Deployment

On-Premises deployment enables organizations to install and operate our applications on their own infrastructure. This approach offers the highest level of control and customization, making it particularly suitable for organizations with strict security, compliance, or performance needs. It is best suited for enterprises with dedicated IT resources and the expertise to manage complex infrastructure. For additional information about on-premises deployment, click here.

Managed Kubernetes Deployment (AKS, EKS, and GKE)

We offer support for deployment on Managed Kubernetes services such as Amazon EKS, Microsoft AKS, and Google GKE. Managed Kubernetes platforms simplify the management of Kubernetes clusters by handling tasks like cluster provisioning, maintenance, and scaling.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

This deployment option is suitable for organizations looking for a balance between control and operational simplicity, and for those who prefer leveraging cloud providers' infrastructure and expertise. For additional information about managed kubernetes deployment, click here.

- Key Capabilities of CERT+
- Start with Your Onboarding Journey
- CERT+ Requirement and Access
- RBAC Configuration
- Enabling RBAC for CERT+ Native Workflows
- Invite Teammates to Your AppViewX Trial

Key Capabilities of CERT+

A single pane management interface for end-to-end Certificate and Key management, automation, and Orchestration:

Discovery and Visibility

An administrator can use CERT+ to identify certificates by scanning networks to fetch certificates from AppViewX-managed servers, devices, or certificates.

- Discover unknown certificates and keys across heterogeneous environments.
- Group certificates and keys, apply access restrictions and assign governance policies.
- Monitor expired certificates, notify, and renew certificates on time.
- Get a holistic view of certificates, keys, and respective device associations.

Inventory and Management

AppViewX Certificate Inventory serves as a repository for all certificates that have been discovered, uploaded, or enrolled via AppViewX. Administrator can configure role-based access control for these certificates by using Certificate Groups.

Dashboard for Visibility and Monitoring

The dashboard in AppViewX provides a comprehensive view of certificates and certificate hosting infrastructure. It enables users to gain insights into the PKI infrastructure, monitor expiring certificates, and assess security posture. Users can also configure custom widgets to create business-specific views of the certificate infrastructure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CLM Automation

Certificate automation allows you to automate the certificate lifecycle process across your enterprise using a configurable workflow engine. The platform can automate and orchestrate not only CLM actions but also configure change and process automation as defined by organizational processes.

- Access to a catalog of advanced automation workflows for certificate management.
- Build custom, event-driven automation using pre-built workflow tasks.
- Self-service automation workflows for easier policy-based certificate enrollment.
- Certification enrollment allows users to generate a CSR, get a CSR signed by a CA, renew or regenerate a certificate, and reissue a certificate.
- Certificate provisioning pushes a certificate to the device and binds it to the application configurations.
- Users can leverage additional management actions like revoke a certificate, migrate certificates from one CA to another through CA switch, check for revocation status of a certificate using OCSP and SSL checker to validate the deployment of a certificate.
- Integrate with ITSM, ChatOps tools for holistic Incident and Change management, and notifications.
- Enforce custom expiration dates or enable auto-rotation of keys.

Cloud and DevOps

- Discover, manage and automate certificates across multi-cloud and container environments.
- Generate internal certificates for test applications before migrating to external certificates.
- Request any certificate and provision it to cloud key stores using a single interface.
- Manage certificate enrollment and availability on Vault Keystores for containerized environments.
- ACME for easier certificate enrollment.

Secure Key Management

- Encrypt and secure private keys in a FIPS-compliant database and secure encryption keys on a vault or a FIPS 140-2 certified HSM.
- Use a built-in or third-party password vault to store critical passwords.
- Avoid Private Keys on wire by generating them directly on the device.

Certificate and Key Compliance

- Standardize certificate provisioning using self-service.
- Enforce organization standards through policies for compliance.
- Define granular role-based access control and enforce business-specific policies.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Create audit trails for each user and certificate or key-related activity.
- Get the certificate and key logs on SIEM dashboards.

IoT and Enterprise Mobility Certificate Management

- Get a single SCEP and EST for enrollment requests from IoT and network end-points.
- Integrate with EMM/MDM systems and self-service certificate issuance using SCEP.
- Intune SCEP for systems managed through Azure Intune.
- Standardize certificate management across multivendor platforms.
- Use out-of-box integration with vendors to handle certificate provisioning.

SSH Key Lifecycle Automation

- Discover SSH keys from Linux and Windows machines
- Enforce timebound access to servers by managing keys on both client and server machines.
- Discover non complaint keys or hosts not following organization standards.
- Report long existing accesses to be revoked.

Alerts & Logs

- CERT+ platform alerts you about certificates expiring within a user-configured time frame.
- CERT+ stores information about events that have occurred or actions performed by a user for certificate lifecycle management.
- CERT+ offers additional alerts to monitor changes to the availability of a certificate on an endpoint.
- CERT+ prevents unexpected certificate expirations by providing alerts and notifications to save time and secure the enterprise network.

Groups & Policies

- The certificates generated or discovered in the CERT+ platform can be logically grouped for ease of management.
- All certificate actions on a specific group can be restricted via role-based access control (RBAC).
- The platform comes prebuilt with a default group to which all the certificates identified from managed devices are associated.
- Groups are similar to a folder that stores a number of certificates with similar components.
- A policy is a set of rules that can be enforced on a certificate group.
- A defined set of certificate parameters can be created as policies.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Policies help in enforcing security compliance over certificate creation across the organization.
- All the certificates discovered and inventoried are compared against the policy to identify non-compliance.

Administration

This feature aids administrative tasks like saving a certificate keystore password into the password vault, configuring auto-enrollment, certificate authority, device management, certificate profile, programmable certificate authority, programmable application endpoint, job scheduler, certificate attributes, email settings, and actions on expired certificates and certificate history.

Start with Your Onboarding Journey

The customer onboarding process involves a trial subscription, initial network integration, and discovery of both public and private CA certificates for centralized management. Automated workflows address issues such as expiring certificates and compliance, enhancing security and visibility while reducing manual effort.

The Onboard Discovery feature in AppViewX automates the management of digital certificates by scanning the network to detect and import SSL/TLS certificates from devices such as servers and load balancers into the AppViewX Trust Protection Platform. This centralizes certificate management and eliminates manual intervention. The platform continuously monitors certificates for status changes, expiration dates, and compliance, automating renewals and deployment to prevent downtime.

For certificate onboarding, freemium/new customers and existing customers will follow different processes.

- **Freemium/New Customers**: Directed to the **CERT+** > **Insights** > **Summary** page, where a pop-up window appears outlining the onboarding journey.
- **Existing Customers**: Directed to the **CERT+** > **Insights** > **Summary** page. Here, a **Quick Discovery** button appears, which redirects them to the onboarding journey.

The **INSIGHTS** menu provides comprehensive information and analytics regarding the overall certificates summary, operations, Risk & Crypto, and Google 90-Day delivered through the CERT+ infrastructure. The INSIGHTS menu populates with relevant data, once the certificates have been successfully onboarded and discovered. For more details about Insights, refer to Insights section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Subscribe AppViewX Trial Application
- Onboarding Journey
- Remediate Certificate Issues

Subscribe AppViewX Trial Application

The AppViewX trial application is a limited-access version of the AppViewX platform designed to allow potential customers to explore and evaluate its features and capabilities. By subscribing to the trial application, you can test functionalities such as certificate management, CA discovery, and remediation of certificate issues without committing to a full purchase. You can gain hands-on experience with AppViewX's capabilities and determine how well it fits your organization's needs.

Note: If you have already subcribed for the trial application, skip this procedure and proceed with the Onboarding Journey.

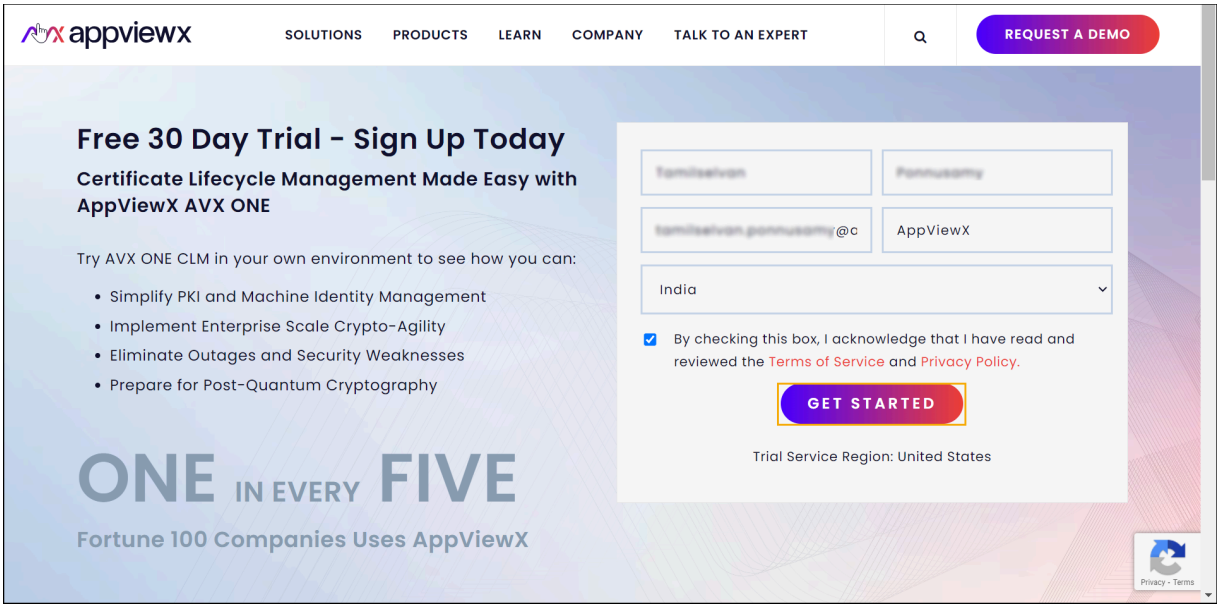
To subscribe AppViewX trial application,

1. Launch your preferred web browser, and then enter the AppViewX website URL.

   The AppViewX home page is displayed.

2. Click the **Free Trial** button.

   The **Free Trial** page is displayed.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter the required details in the field such as **First Name**, **Last Name**, **Business Email**, and **Company Name**.

> **Note:** *: Mandatory fields

4. Select the country name from the **Select Country** dropdown list.
5. Click **GET STARTED**.
6. You will receive an email for the confirming your email address.
7. Click the **GET STARTED** button from the email.
8. Your email address will be verified.

> **Note:** Once you sign up, it takes a few minutes to create a tenant and send a welcome email to the provided email address.

9. You will get a welcome email.

   The email subject as **Welcome to your Free AppViewX <on-prem or SaaS> Trial**.

10. The email contains **Login URL**, **Username**, and **Temporary Password**.
11. Click the **login** URL.

    The **Sign in** page is displayed in the new browser window.

12. Enter the **User name** and then **Password** in its field.

> **Note:** For example,
> • **User name**: test.test@appviewx.com
> • **Password**: Temporary password that has been received via email.

13. Click **Sign in**.
14. The **Change password** page is displayed.
15. Enter your new password in the **New Password** field. Ensure that it meets the password requirements. For example, mix of upper and lower case letters, numbers, and special characters).
16. Re-enter your new password in the **Confirm New Password** field to verify it.
17. Click **Continue**.

    The **Change password** page is displayed with the message as Your password has been changed successfully. You will be redirected to login page. Please login again.

18. (or) Click **Back to Login**, to return to the login page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

19. Click the **login** URL in the message.

    You are redirected to **Sign in** page.

20. Enter the valid credential, and then click the **Sign in** button.

    The **Terms of Service** page is displayed.

21. Read the terms and conditions, and then click the check box to **I accept these terms and conditions**.
22. Click **Continue**.

What's Next

- Onboarding Journey
- Remediate Certificate Issues

Onboarding Journey

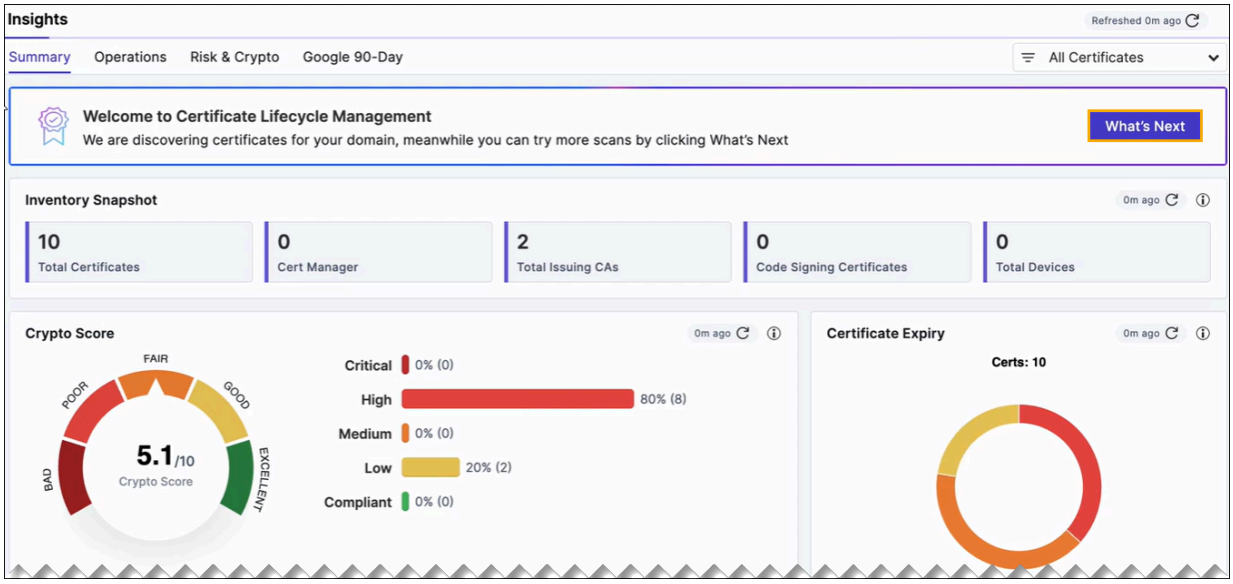
As part of the onboarding process, you have the capability to perform both Public CA Scans and Private CA Scans. These certificate discovery scans play a crucial role in identifying and analyzing digital certificates within your organization. By regularly conducting these scans, organizations can maintain an up-to-date record of their certificates, ensuring that all digital certificates, both public and private, are accurately inventoried and tracked. This facilitates efficient certificate management, including renewal, replacement, and revocation processes. Additionally, these scans help in proactively identifying and addressing any security concerns, such as expired, misconfigured, or vulnerable certificates, before they lead to potential breaches or disruptions.

These scans allow for the identification of high-risk, critical-risk, and non-standard certificates, providing the necessary insights to remediate these issues, thereby improving the overall crypto score and strengthening the organization's security posture. By leveraging these discovery scans, organizations can maintain robust certificate management practices, enhance their security measures, and ensure compliance with relevant regulations, ultimately safeguarding their digital infrastructure and data.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Freemium or New Customers to Initiate the Onboarding Process

- Click the **What's Next** button in the welcome banner that appears on the **Insights** > **Summary** section. For more details about Insights Summary, refer to Insights Summary section.

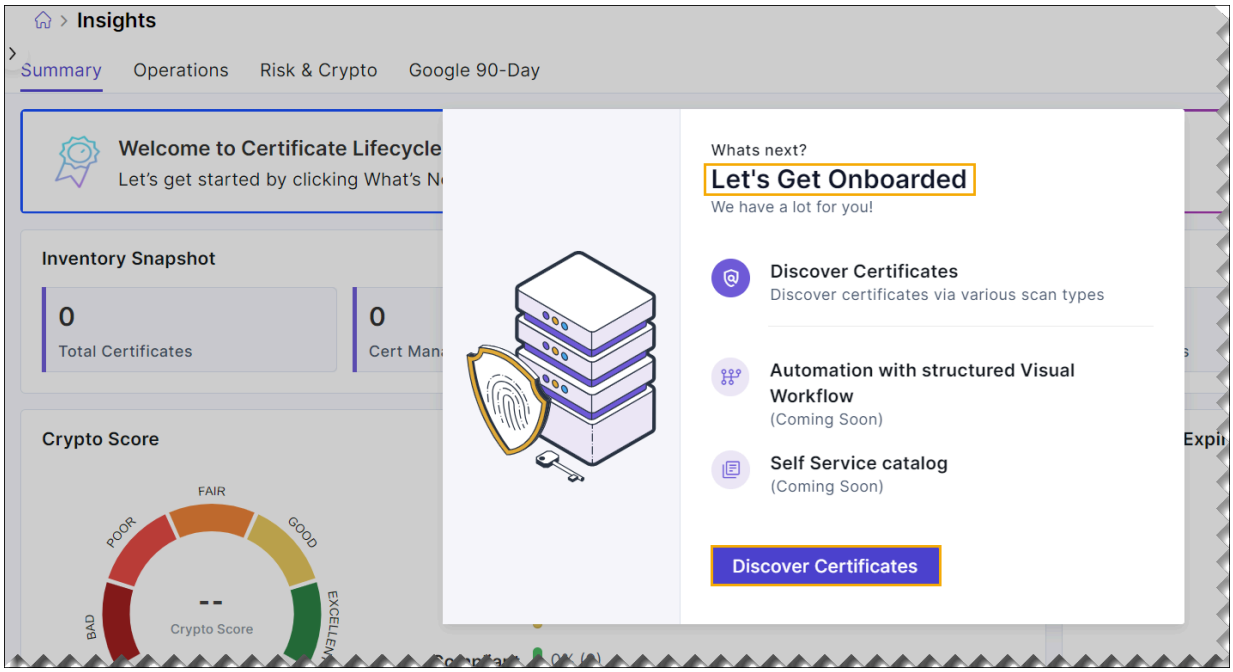


Note:

- The Certificate Transparency (CT) Log Scan is a background process in the CERT + application that continuously monitors and fetches certificate data from Certificate Transparency logs. This scan helps in identifying and managing certificates by bringing the results directly to the Insights Summary page, providing users with real-time visibility into their certificate landscape.
- If the CT Log Scan encounters issues such as a network outage or other disruptions that prevent it from completing its task, the application detects the failure. To ensure users are aware of the issue and to guide them through alternative steps, the application triggers a **Let's Get Onboarded** pop-up window.

- (or) The **Let's Get Onboarded** pop-up window appears in the **Insights** > **Summary** tab.

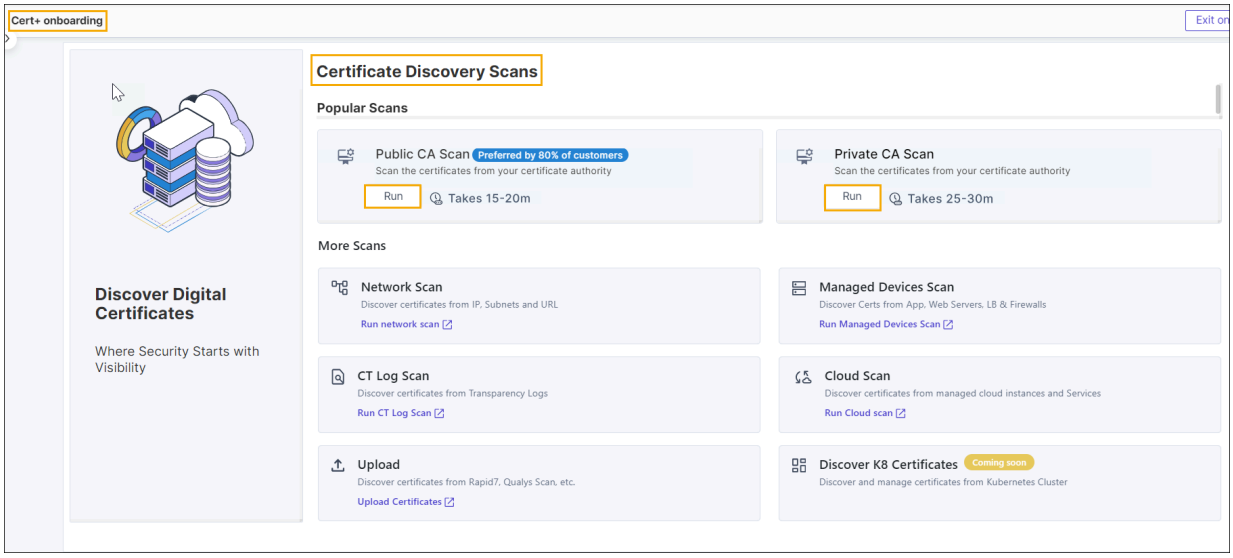
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Note: Once the certificate discovery process is complete, the welcome banner will disappear.

- Click the **Discover Certificates** button from the pop-up window.

The **Cert+ onboarding > Certificate Discovery Scans** page is displayed.

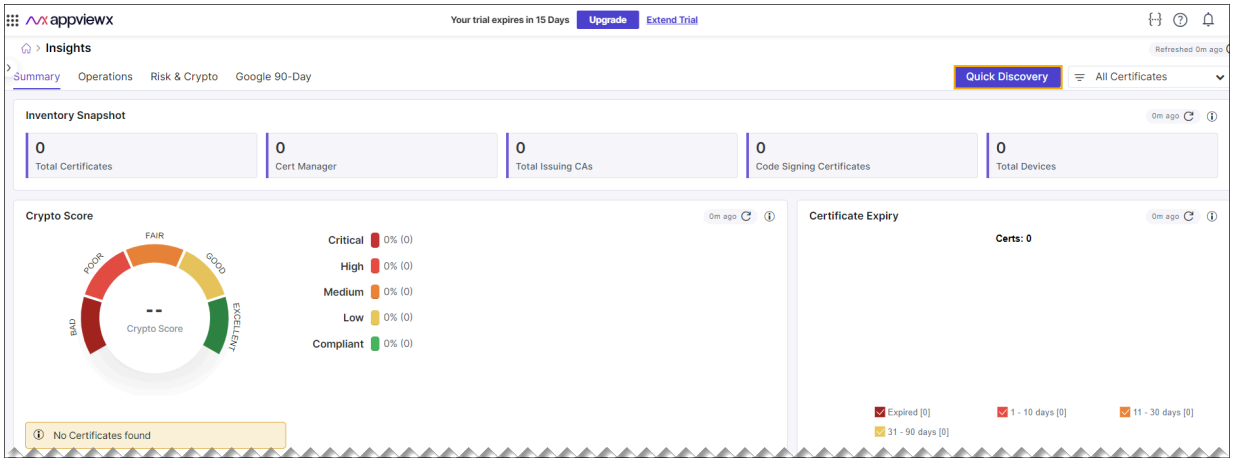


Note: Initially, only popular scans **Public CA Scan** or **Private CA Scan** will be enabled. More scans will become available once you try one of the popular scans.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

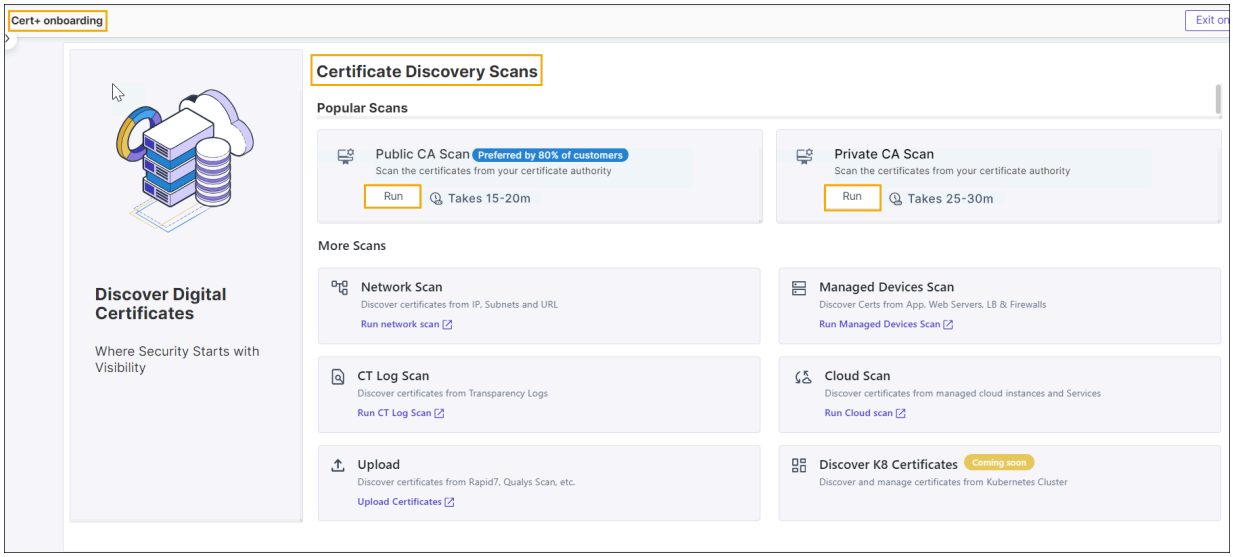
Existing Customers to Initiate the Onboarding Process

- Click the **Quick Discovery** button that appears on the **Insights** > **Summary** section. For more details about Insights Summary, refer to Insights Summary section.



Note: The Certificate Transparency (CT) Log Scan is a background process in the CERT+ application that continuously monitors and fetches certificate data from CT logs. This scan helps in identifying and managing certificates by bringing the results directly to the Insights Summary page, providing users with real-time visibility into their certificate landscape.

The **Cert+ onboarding > Certificate Discovery Scans** page is displayed.



Note: Initially, only popular scans **Public CA Scan** or **Private CA Scan** will be enabled. More scans will become available once you try one of the popular scans.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Public CA Scan

A public CA is a third-party organization that issues certificates for a fee after performing required checks on the requesting organization. These checks typically include domain validation. Public CAs use their own public-private key pairs to sign the certificates.

As part of the onboarding process, you can perform Public CA Scans targeting certificates issued by public Certificate Authorities (CAs) such as **DigiCert** and **Entrust**. These scans identify and analyze digital certificates within your organization's infrastructure, ensuring a complete inventory, timely renewal, security compliance, and proactive vulnerability remediation. They analyze certificate configurations, highlight high-risk, critical-risk, and non-standard certificates, and maintain detailed records. By leveraging these scans, organizations can effectively manage their certificates, ensure security and compliance, and safeguard their digital infrastructure while maintaining stakeholder trust.

DigiCert CA Scan

Prerequisites

- Make sure that you have DigiCert API key.
- To obtain the DigiCert API key, follow the instructions provided on the **Prerequisites Public Scan** page.

1. In the **Public Scan** section, click **Run**.

   The **Prerequisites Public Scan** page is displayed.

2. Click **DigiCert** from the **Vendors** left menu.

   > **Note:** Complete the instructions provided on the **Prerequisites Public Scan** page.

3. Click **Close** to return to the **Cert+ onboarding** page.

For the **DigiCert** CA discovery scan, follow these steps.

1. In the **Discovery Details** section,
   a. Enter the **Discovery Instance Name** in the field.

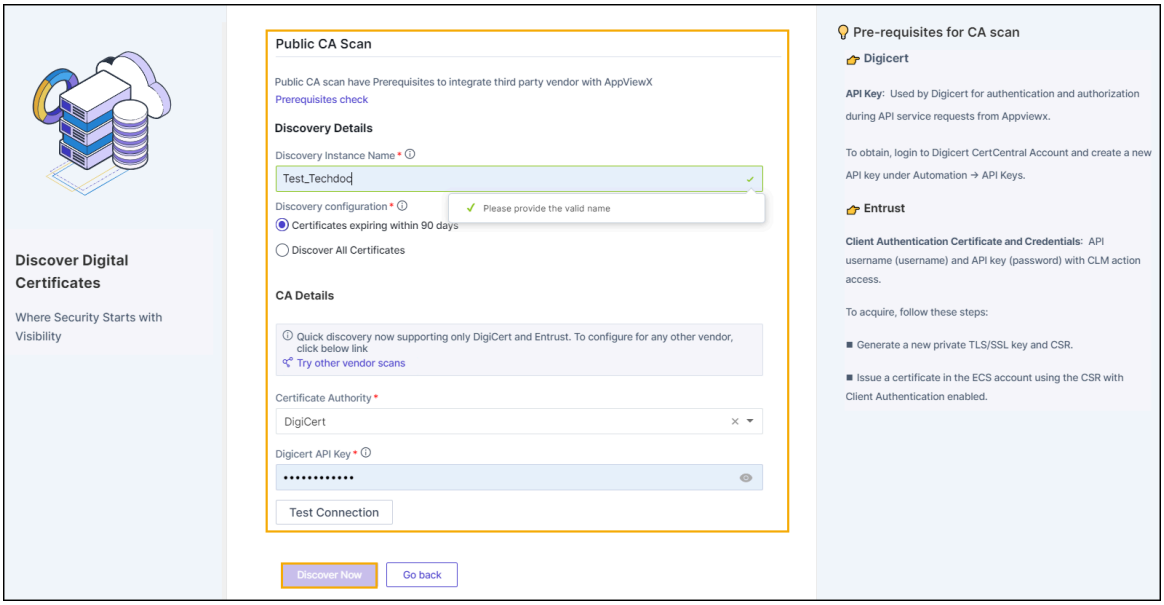
   > **Note:** The instance name can be any friendly name to the scan configuration.

   b. Click the required radio button for the discovery configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The available **Discovery configuration** options are,

- **Certificate expiring within 90 days**: By configuring the certificate expiring within 90 days feature, the discovery scan and monitoring will happen faster, allowing organizations to efficiently manage their digital certificates and ensure strong security and smooth operations.
- **Discover all certificates**: By configuring the Discover all certificates feature, the discovery scan might take longer depending on the certificate volume, with the time varying based on the number of certificates.



Note: By default, the **Certificates expiring within 90 days** radio button is enabled.

2. In the **CA Details** section,
   a. Select the **Certificate Authority** as **DigiCert** from the dropdown list.
   b. In the **Digicert API Key** field, enter the API key.
3. Click the **Test Connection** button.
4. Click the **Discover Now** button.

Entrust CA Scan

Prerequisites

- Client Authentication Certificate
- API username (username)
- API key (password) with CLM action access

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- To obtain the Entrust prerequisites, follow the instructions provided on the **Prerequisites Public Scan** page.
  1. In the **Public Scan** section, click **Run**.

     The **Prerequisites Public Scan** page is displayed.
  2. Click **Entrust** from the **Vendors** left menu.

     Note: Complete the instructions provided on the **Prerequisites Public Scan** page.
  3. Click **Close** to return to the **Cert+ onboarding** page.

For the **Entrust** CA discovery scan, follow these steps.

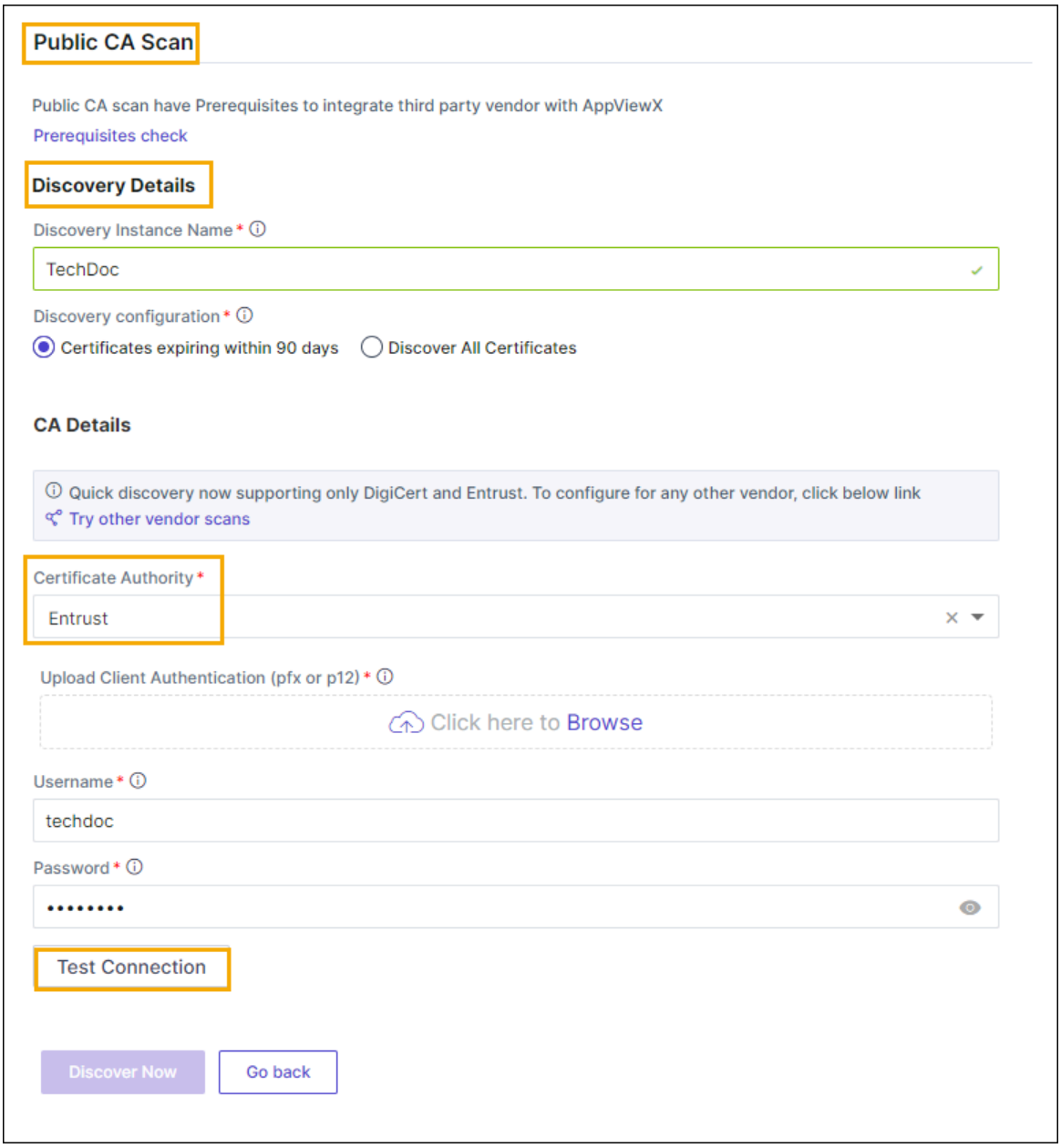
1. In the **Discovery Details** section,
   a. Enter the **Discovery Instance Name** in the field.

      Note: The instance name can be any friendly name to the scan configuration.

   b. Click the required radio button for the discovery configuration.

      The available **Discovery configuration** options are,
      - **Certificate expiring within 90 days**: By configuring the certificate expiring within 90 days feature, the discovery scan and monitoring will happen faster, allowing organizations to efficiently manage their digital certificates and ensure strong security and smooth operations.
      - **Discover all certificates**: By configuring the Discover all certificates feature, the discovery scan might take longer depending on the certificate volume, with the time varying based on the number of certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Note: By default, the **Certificates expiring within 90 days** radio button is enabled.

2. In the **CA Details** section,
   a. Select the **Certificate Authority** as **Entrust** from the dropdown list.
   b. Click the **Browser** button to upload the client authentication. Allowed formats are <**.pfx**> or <**.p12**>.
   c. Enter the API username to communicate with CA in its field.
   d. Enter the API password to communicate with CA in its field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click the **Discover Now** button.
4. Click the **Test Connection** button.

Private CA Scan

When an organization creates its own local CA instead of using an external one, it is referred to as a private CA. In this case, the certificates are signed with the private key of the organization's root certificate, which is the primary certificate used to sign other certificates. Private CAs can be established to issue certificates for an organization's internal network, where discretion is required and only a select group of users are involved.

As part of the onboarding process, you can perform Private CA Scans targeting certificates issued by private Certificate Authorities (CAs) such as Microsoft. These scans analyze and identify digital certificates across your organization, ensuring a thorough inventory, timely renewal, security compliance, and proactive vulnerability management. They assess certificate configurations, flag high-risk, critical-risk, and non-standard certificates, and maintain comprehensive records. By utilizing these scans, organizations can efficiently manage certificates, uphold security standards, protect digital infrastructure, and maintain stakeholder trust.

Microsoft CA Scan

Prerequisites

- Cloud Connector: Install on a Linux system with minimum requirements: 4CPU, 8GB.
- Command Execution Host: A Windows system attached to the Microsoft CA for cloud connector connection and scan execution.
- Username/Password: Credentials for accessing the command execution host.
- CA Machine Host Name: Automatically populated based on the selected CA.

Note: Use IP if hostname resolution fails from cloud connector.

For the **Microsoft** CA discovery scan, follow these steps.

1. In the **Discovery Details** section,
   a. Enter the **Discovery Instance Name** in the field.

Note: The instance name can be any friendly name to the scan configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. In the **Connectivity** section, click the Cloud Connector dropdown menu.
3. Click the **+Add New** button.

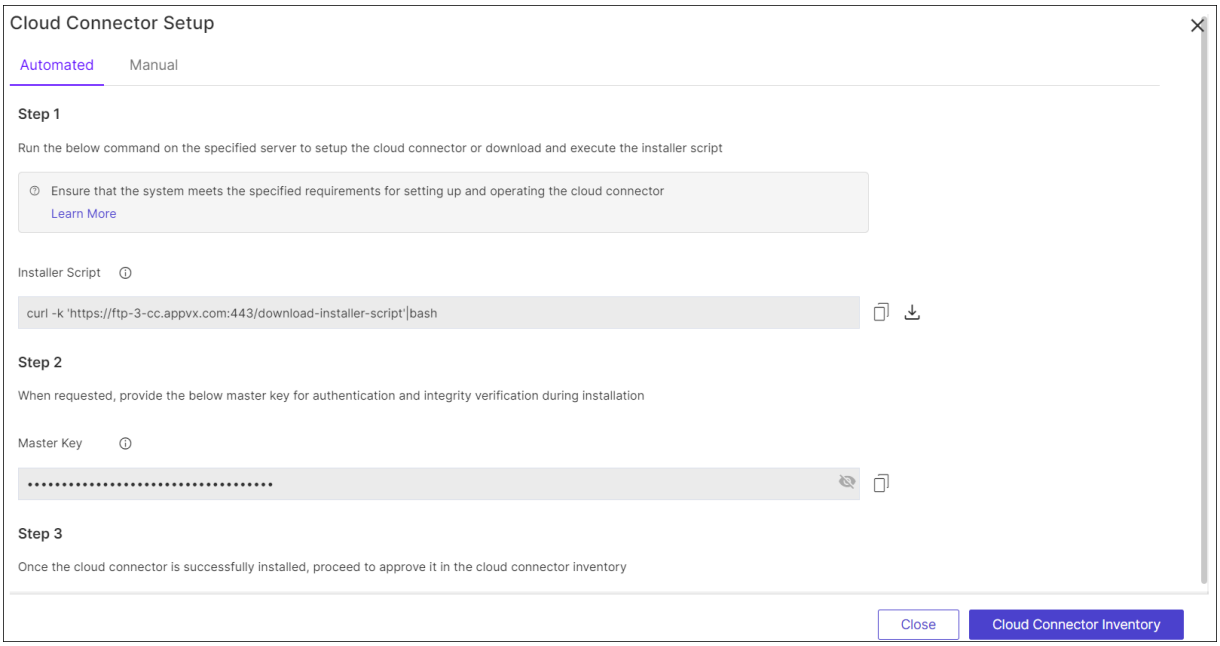
The **Cloud Connector Setup page** is displayed. For more details, refer Cloud Connector User Guide.

The cloud connector (CC) can be connected with private CA in two ways.

- Automated
- Manual.

Note: By default, the **Automated** tab is selected.

For the automated CC connection with private CA, follow these steps.



a. Run the below command on the specified server to setup the cloud connector or download and execute the installer script.

```
curl -k 'https://ftp-3-cc.appvx.com:443/download-installer-script'|bash
```

b. When requested, provide the below master key for authentication and integrity verification during installation.

```
22f77628-51c6-4209-b59f-3c91f859ea63
```

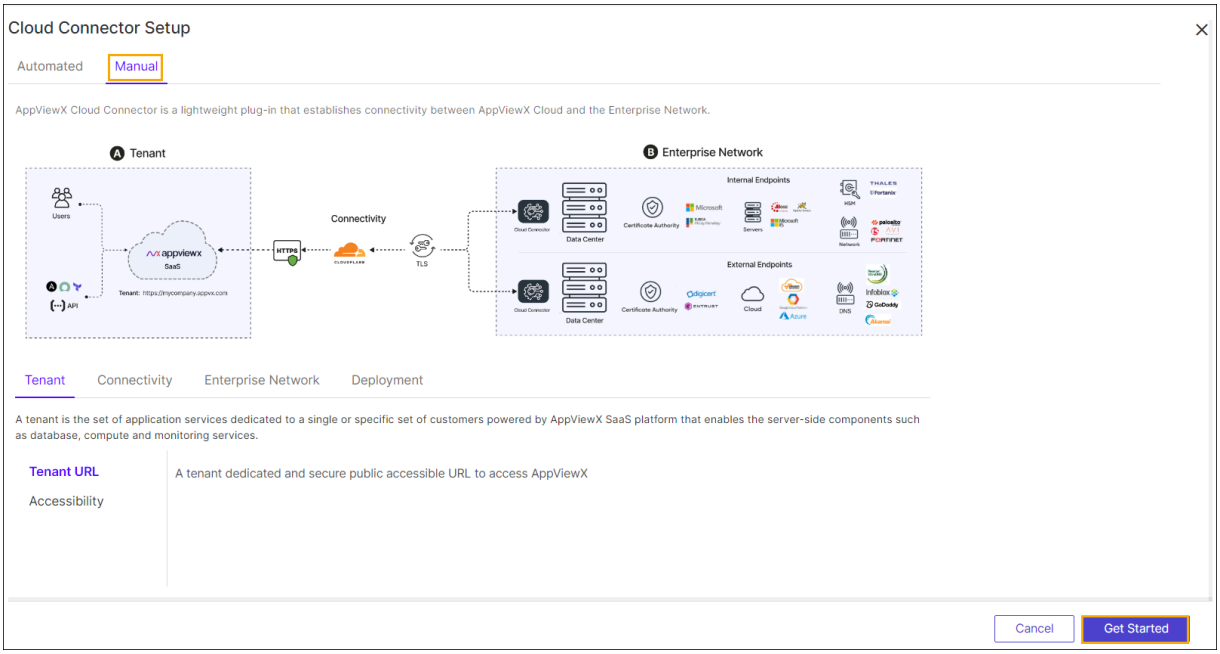
c. Once the cloud connector is successfully installed, proceed to approve it in the cloud connector inventor.
d. Click **Cloud Connector Inventory**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Setting Cloud Connector** page is displayed.

e. Click **Close**.

(or) **For the Manual CC connection with private CA, follow these steps.**



a. Click **Get Started**.

The **Basic Information** page is displayed. For more details, refer Cloud Connector User Guide.

i. Select the desired **Installation Type** radio button.
   - Native OS
   - Virtual Image.

ii. Enter the Cloud Connector Name (FQDN) in the field.

b. Click **Next**.

The **Assign Data Center** page is displayed.

i. Click Add Data Center.

The **Add Data Center** page is displayed.

ii. Enter the name of the data center in the field.

c. Click **Next**.

The **Advanced Configuration** page is displayed.

i. Select the TLS Authentication radio as required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*TLS Authentication	The available TLS Authentications are: • Auto Generate • Custom Certificate By default, **Auto Generate** is selected.
*TLS Certificate Password	Enter the TLS certificate's password.
*TLS Certificate	Upload TLS certificate in the <.p12> format.
*: Mandatory fields	

d. Select the **Use Proxy** check box if required.

e. Select the proxy from the dropdown list.

i. If not listed in the dropdown menu, click **Click here** link.

The Add Proxy page is displayed.

ii. Enter/select the following details **Proxy Name**, **Server IP**, **Port**, **URL**, **Authentication**, **Username**, and **Password** in the Add Proxy page

iii. Click **Save**.

4. Click **Finish**.
5. Click the **Test Connection** button, to validate the connection.
6. Click the **Discover Now** button.

What's Next

- Remediate Certificate Issues

Remediate Certificate Issues

Remediating certificate issues involves identifying and resolving problems related to digital certificates within an organization's infrastructure. By regularly deleting expired and revoked certificates, regenerating high-risk and critical-risk certificates with enhanced parameters, and renewing or regenerating certificates nearing expiration, organizations can significantly improve their crypto score. This proactive approach ensures robust cryptographic security, compliance with industry standards, and a well-maintained certificate infrastructure, ultimately safeguarding digital assets and maintaining stakeholder trust.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Delete Expired and Revoked Certificates from Inventory

Expired and revoked certificates pose significant security risks as they can no longer provide the necessary cryptographic protection. To improve your crypto score:

- **Identify Expired Certificates:** Regularly scan your inventory to detect certificates that have passed their expiration date.
- **Remove Expired Certificates:** Delete these expired certificates from your system to prevent any potential misuse.
- **Identify Revoked Certificates:** Similarly, identify any certificates that have been revoked due to compromise or other reasons.
- **Remove Revoked Certificates:** Ensure that revoked certificates are promptly removed from your inventory to maintain security integrity.

Regenerate High-Risk and Critical-Risk Certificates

High and critical-risk certificates typically have vulnerabilities or weak cryptographic parameters. Regenerating these certificates with enhanced security settings is crucial.

- **Identify High and Critical-Risk Certificates:** Use your certificate management system to identify certificates flagged as high or critical risk.
- **Review Risk & Crypto Settings:** Access the Risk & Crypto settings in your management system to understand the parameters required for secure certificate regeneration.
- **Regenerate Certificates:** Follow these steps to regenerate the identified certificates:
  - Generate new keys with stronger encryption algorithms (e.g., using RSA with a 2048-bit key or ECC with a recommended curve).
  - Ensure the use of longer key lengths and secure hashing algorithms.
  - Implement certificate policies that align with industry standards and best practices.
- **Deploy New Certificates:** Replace the old certificates with the newly generated ones in your infrastructure.

Renew or Regenerate Certificates That Are About to Expire

To maintain continuous security and avoid service disruptions, it’s essential to renew or regenerate certificates nearing their expiration date.

- **Identify Certificates Near Expiration:** Regularly monitor your certificate inventory to find those that are approaching their expiration dates.
- **Renew Certificates:**

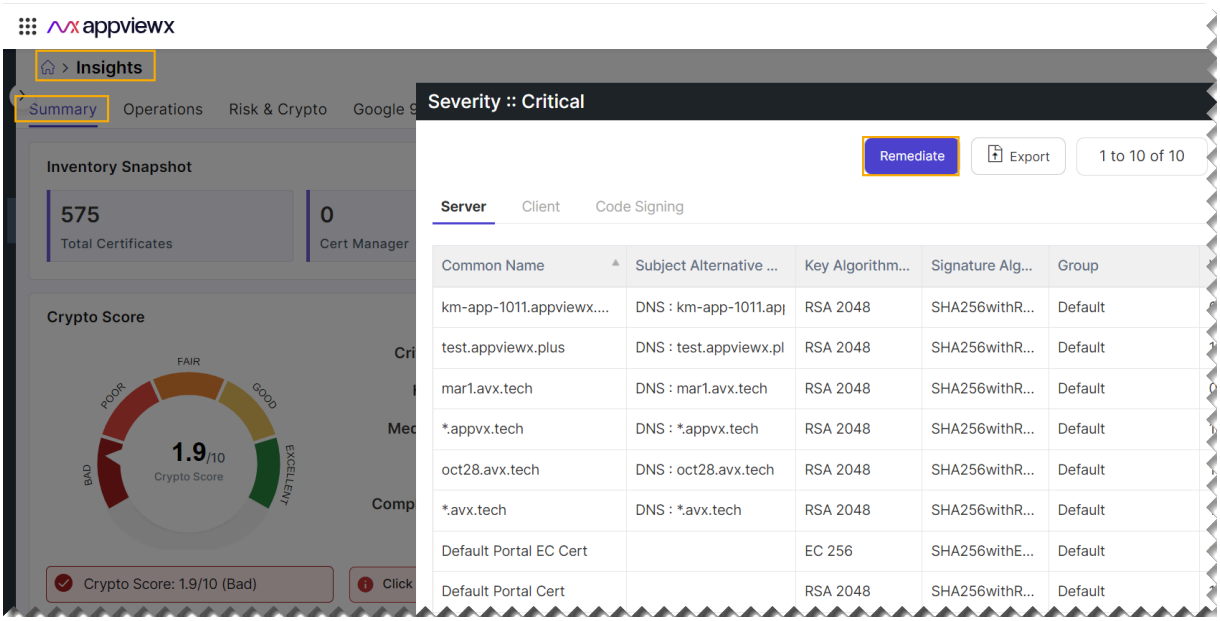
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Contact the issuing Certificate Authority (CA) to renew the certificates.
- Follow the CA's renewal process, ensuring that the renewed certificates meet your security requirements.

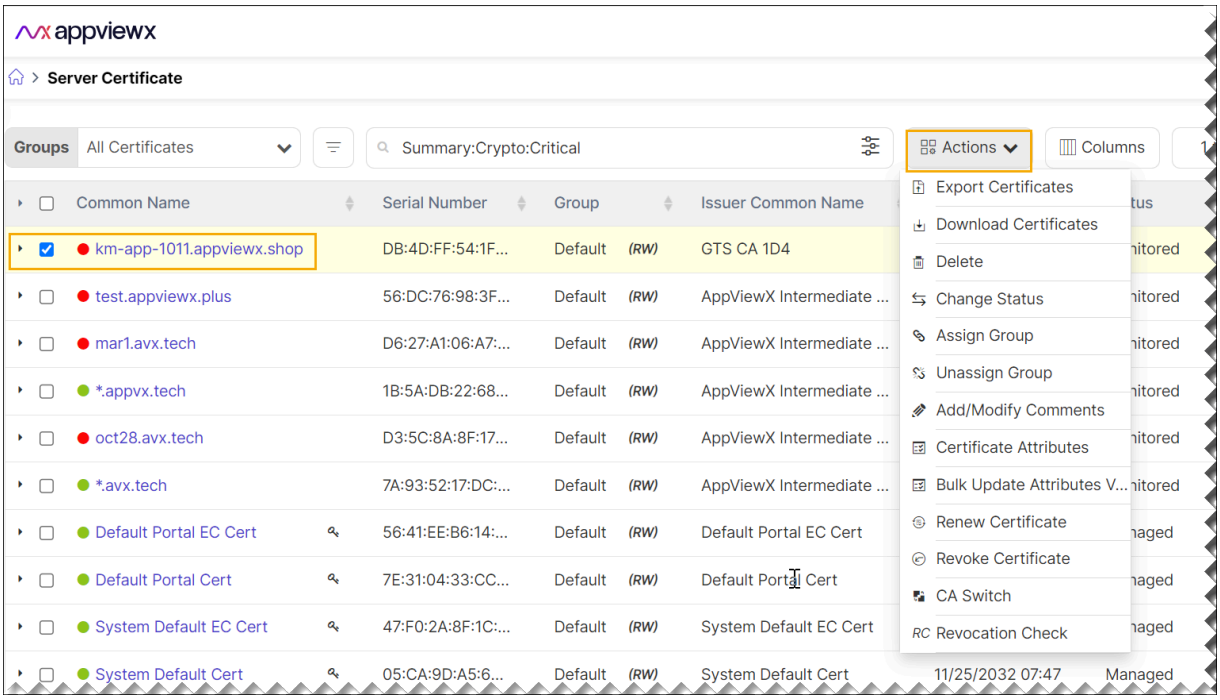
- **Regenerate Certificates:** If renewal is not possible or practical, regenerate new certificates using updated cryptographic parameters as described above.
- **Deploy Renewed/Regenerated Certificates:** Ensure that the newly renewed or regenerated certificates are deployed across all relevant systems and applications before the old ones expire.

Check Certificate Expiry

1. Navigate to **Insights** > **Summary** > **Crypto Score** section.
2. Click **Critical** or **High** priority certificate in the chart that takes to intermediate page.
3. Click the **Remediate** button to redirect to the Server/Client/Code signing certificate inventory.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Note: It allows you to initiate the renewal or replacement process for these certificates.

4. Take necessary actions for critical and high-priority certificates. For more details about CLM inventory actions, refer to the Managing the Certificate Inventory.

Remediate Non-Standard Certificate

Effective remediation of non-standard certificates is essential for maintaining a secure and compliant digital infrastructure. By regenerating self-signed certificates with trusted CAs, replacing wildcard certificates with individual domain certificates, verifying or deleting unknown certificates, issuing certificates from intermediate rather than root CAs, correcting SAN mismatches, and associating all certificates with their intended devices, organizations can significantly enhance their security posture and ensure adherence to industry best practices.

Self-Signed Certificates

Issue:

- Self-signed certificates are not issued by a trusted Certificate Authority (CA) and are typically used for internal testing or small-scale applications.

Remediation:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Regenerate the Certificate from a Trusted CA:** Replace self-signed certificates with ones issued by a trusted CA. This ensures that the certificates are recognized and trusted by other systems and browsers, thereby enhancing security and trust.

Self-Signed Certificates

Issue:

- Self-signed certificates are not issued by a trusted Certificate Authority (CA) and are typically used for internal testing or small-scale applications.

Remediation:

- **Regenerate the Certificate from a Trusted CA:** Replace self-signed certificates with ones issued by a trusted CA. This ensures that the certificates are recognized and trusted by other systems and browsers, thereby enhancing security and trust.

Wildcard Certificates

Issue:

- Wildcard certificates are used to secure multiple subdomains with a single certificate. While convenient, they can pose security risks if compromised, as they grant access to multiple subdomains.

Remediation:

- **Create Individual Certificates for Each Domain:** Instead of using a wildcard certificate, generate individual certificates for each subdomain. This limits the scope of any potential security breach to a single subdomain.

Unknown Certificates

Issue:

- Certificates issued by unknown or untrusted entities can’t be verified for their authenticity and may pose security risks.

Remediation:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Trust the Issuers or Delete the Certificates:** Verify the legitimacy of the issuing entity. If the issuer is trustworthy, add them to your list of trusted entities. If the issuer cannot be verified, delete the certificates to avoid potential security risks.

Root CA Issued Certificates

Issue:

- Certificates issued directly by a root CA are typically less secure than those issued by an intermediate CA, as they do not follow the recommended hierarchical trust model.

Remediation:

- **Regenerate the Certificates from a Trusted Intermediate CA:** Replace root CA-issued certificates with certificates issued by a trusted intermediate CA. This follows the best practice of using a hierarchical trust chain, improving overall security.

Subject Alternative Name (SAN) Mismatch

Issue:

- SAN mismatch occurs when the certificate's SAN fields do not match the actual Fully Qualified Domain Name (FQDN) it is supposed to secure.

Remediation:

- **Enroll New Certificates for the Actual FQDN:** Generate new certificates that correctly list the intended FQDNs in the SAN field. Deploy these new certificates to ensure they match the domain names they are intended to secure, preventing security warnings and potential man-in-the-middle attacks.

Unassociated Certificates:

Issue:

- Unassociated certificates are those that are not currently linked to any device or service within your infrastructure, leading to potential management and security gaps.

Remediation:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Manage Respective Devices to Associate Certificates:** Identify the intended devices or services for these certificates and properly associate them. This ensures that all certificates are actively managed and utilized, reducing the risk of forgotten or unused certificates that could lead to security vulnerabilities.

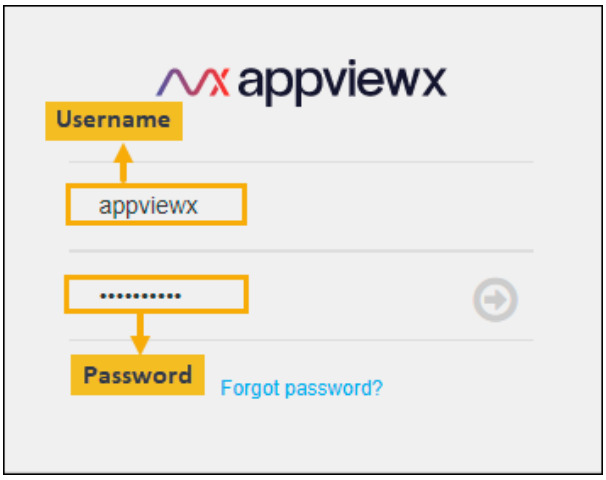
CERT+ Requirement and Access

Supported Web Browsers

Web Browser	Version
Firefox	128 (64-bit) or later
Google Chrome	127 (64-bit) or later

Accessing the CERT+

1. Log in to AppViewX with a valid credential.
   The AppViewX Landing page appears.



2. Click (**Menu**) button located in the upper left corner of the screen.

> **Note:** The product URL will be shared by AppViewX in the onboarding emails.

3. Click **CERT+** on the left navigation bar.
   The CERT+ home page is displayed, and the menu will be updated to the CERT+ menu.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Licensing Models

The licensing for CERT+ is done using two models:

- Certificate Instance Based Model
- Certificate Count Based Model (introduced in v2023.1.0 FP3)

You can choose the certificate licensing model at the time of requesting for a license.

Certificate Instance Based Model

In this model, the certificate count is the number of connectors associated with a certificate.

Certificate count is derived using the following logic:

- If a certificate has one non-sync and two certificate connectors, **certificate count = two**.
- If a certificate has one Kube and two certificate connectors, **certificate count = two**.
- If, for a certificate, only the Kube service exists and there are no cert connectors, the certificate will not be counted under the CERT+ license.
- Expired and revoked certificates are included in the certificate count.
- Certificates for which **EKU** = **Server Authentication**/**Server and Client Authentication** are categorized and counted under server certificates.

  Certificates for which **EKU** = any value other than the above two are categorized and counted under device certificates.
- Trial licenses use the certificate instance based model.

The following is a screenshot of an existing CERT+ license page where:

- Managed Certificate includes all Managed certificates (Server, Client, Code Signing and OTHERS)
- Monitored Certificates include all Monitored certificates (Server, Client, Code Signing and OTHERS)
- Managed Server Certificates Instances includes ONLY Managed Server Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Count Based Model

(Introduced in v2023.1.0 FP3)

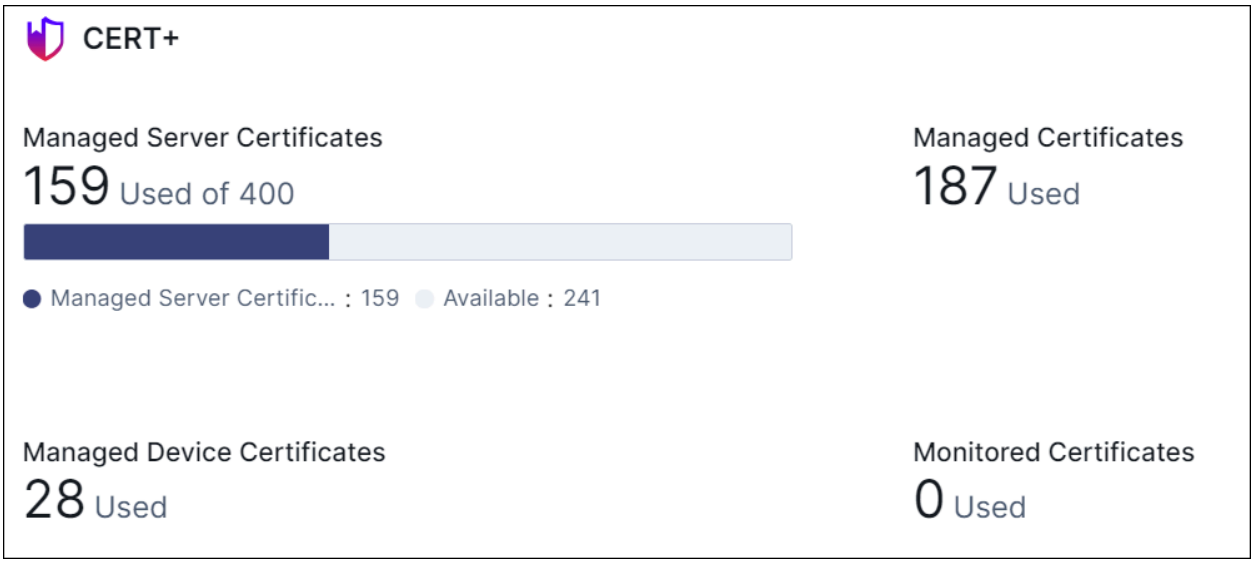
In this model, certificate count is the actual number of certificates in the inventory. Each certificate will be counted as one irrespective of any number of connectors associated with it. Additionally, in comparison with the certificate instance based model, the following changes have also been made:

- Expired and revoked certificates can be moved from Managed to Monitored.
- Once a certificate has been renewed, it can be moved from Managed to Monitored.
- Certificates issues via auto-enrollment will be added in the inventory as Monitored.
- Certificates issued via PKIaaS will be added in the inventory as Monitored, by default.

The following is a screenshot of an existing CERT+ license page, based on the new model, where:

- Managed Certificate includes all Managed certificates (Server, Client, Code Signing and OTHERS)
- Monitored Certificates include all Monitored certificates (Server, Client, Code Signing and OTHERS)
- Managed Server Certificates Instances includes ONLY Managed Server Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



RBAC Configuration

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC) and integrates with existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and Resources can be customized to suit any organizational structure and any user requirements.

Role-based access control (RBAC) is a method of restricting AppViewX functions, network resources that can be managed and monitored in AppViewX based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the AppViewX functions and network resources they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

The Account module enables you to create and manage resources, roles, user groups, and users which are used to ensure that the system:

- Verifies the identity of users logging in to the system **(Authentication)**.
- Controls user access to system resources **(Authorization)**.

Benefits of RBAC

Using RBAC should improve operational efficiency, enhance compliance, provide administrators increased visibility, reduction in costs, decrease in risk of breaches, and data leakage.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Simplified RBAC Configuration in AppViewX

To simplify the existing RBAC Configuration in AppViewX for the Account Administrator, the **Quick Config** wizard flow option has been introduced in the existing Authentication, User groups, Roles, and Resources. Using the **Quick Config** option, users should be able to perform all the following actions in the same wizard flow:

- Configure external authentication or single-sign-on for users to log in to AppViewX.
- Add users groups into AppViewX by pulling specific user groups from AD into AppViewX based on specific patterns/keywords/codes and support the Bulk Export/Import option to onboard user groups.
- Pre-packaged roles for ADC, Cert, Security, and Automation modules to assign permissions to user groups.
- Simplifying custom role creation by providing information help against each ACF explaining the significance of the functionality.
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query or using a script, and assigning permissions to user groups dynamically.

For details on configuring the role and RBAC refer to the **Platform User Guide** > **Configuring Role and Resource-Based Access Control** section.

Enabling RBAC for CERT+ Native Workflows

Native workflows are built-in, automated processes designed to integrate with the UI-based CLM actions to manage the complete lifecycle of digital certificates in a structured, policy-driven manner.

To be able to execute a CLM action from the AppViewX UI, users are required to have the requisite access to the corresponding native workflow.

Native Workflows in CERT+

Native Workflow	CLM Action
certificate_new_request	Enroll certificate
certificate_renew_request	Renew certificate
certificate_new_request	Regenerate certificate
certificate_reissue_request	Reissue certificate
certificate_revoke_request	Revoke certificate

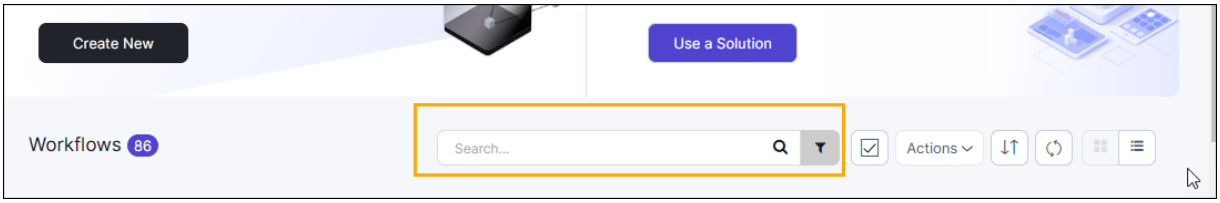
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Native Workflow	CLM Action
certificate_reinstate_request	Reinstate certificate
certificate_suspend_request	Suspend certificate

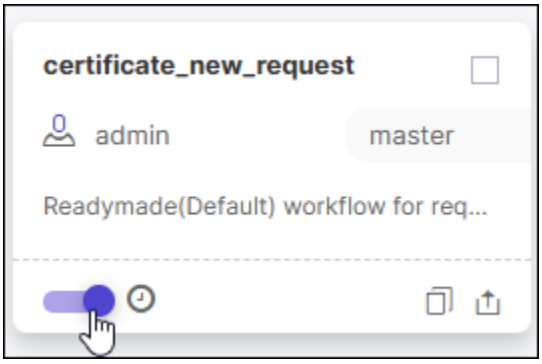
Enabling RBAC for CERT+ Native Workflows

Note: The following process is the same for all native workflows.

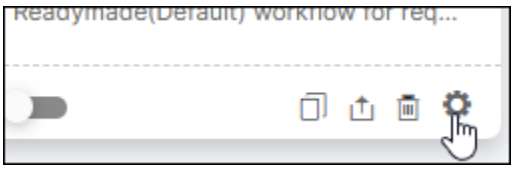
1. Login to AppViewX and go to (**Menu**) > **Automation** > **Workflow** > **Design**.
2. In the **Search** field, enter the name of the workflow you want to enable RBAC for.



3. Turn off the toggle button to disable the workflow before editing it.



4. To open the workflow settings, click .



The **Settings :: <workflow name>** dialog box is displayed.

5. Under the **General** tab, select **Assign workflow**.
6. From the list of resources displayed on the right, for the required resource, click **RW**.

This will enable the read-write permission for the selected resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Click **Save**.
8. Under the **RBAC** tab:

   a. Go to **CSR Submission Request** and, for the required resource, click **S**.
   This will enable the CSR submit permission for the resource.

   b. Click **Save**.

   c. Go to **Approval** and, for the required resource, click **RW**.
   This will authorize the resource to grant Level 1 approval for the request to perform the CLM action.

   d. Click **Save**.

   e. Go to **Implementation** and, for the required resource, click **RW**.
   This will authorize the resource to grant Level 1 approval for the request to perform the CLM action.

   f. Click **Save**.

9. Close the dialog box and turn on the toggle button to enable the workflow.

Invite Teammates to Your AppViewX Trial

AppViewX now allows you to invite your acquaintances to explore and test AppViewX in a trial environment.

To do this:

1. Go to (**Menu**) > **CERT+**.
   The **Insights** landing page is displayed.
2. From the top right corner of the screen, click **Invite Users**.
   The **Invite Teammates** dialog box is displayed.
3. Under **Enter Emails & Assign Groups**:
   a. Enter your teammate's **Email** address.
   b. From the dropdown list, select the user group you want to assign the teammate to.
   c. To add the email address of another teammate, click **Add Another Email**.
   d. Repeat the above step to add as many teammates as required.
4. Click **Send Invite**.
   New users will receive login credentials. If the user already exists, they'll be added to the selected user group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 2: CERT+ User Guide

AppViewX CERT+ User Guide offers detailed instructions for users on how to navigate and utilize the CERT+ certificate lifecycle management platform. It includes step-by-step guidance on performing essential tasks such as managing certificates, monitoring their status, and using various features to ensure effective and secure certificate management.

As a nonadmin user, you can perform the following tasks:

- Onboarding Certificates
- Manage Devices
- Certificate Actions
- Managing the Certificate Inventory
- Certificate Reporting and Monitoring
- Alerts and Logs
- Managing Certificates Using Automation Workflows
- Managing Certificates Using AppViewX Terraform Provider
- Standard Practices

Onboarding Certificates

Important: In compliance with recent updates from the CA/Browser Forum S/MIME Baseline Requirements, for DigiCert-issued S/MIME certificates, it is now mandatory to include the first name and last name, or a pseudonym in the subject information during certificate enrollment.

However, in the current implementation:

- The discovery feature does not retrieve these values in the metadata.
- The upload certificate feature is not compatible with this enhancement since it does not have with a direct mapping to the certificate type, unless the certificate is discovered via a Certificate Authority scan.

- Prerequisites for Onboarding Certificates
- Certificate Discovery
- Discovery Status
- Discovery Exclusions

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Discovery Configuration
- Syncing Certificates with Network Devices or Servers

Prerequisites for Onboarding Certificates

- To discover certificates from managed devices, the device must be managed under the AppViewX Device Inventory.
- To discover certificates from a CA, the CA account should be determined under the AppViewX Certificate Authority settings and network access should be considered.
- AppViewX discovery agent role and usage. For more details, refer to Roles section in the Platform Guide.

Certificate Discovery

Certificate discovery is the process of finding certificates existing in an enterprise network. The first mitigation step to address the certificate expiry outages is to get visibility over the existing certificates and host information in the infrastructure. AppViewX CERT+ enables you to detect risk by discovering all the certificates hosted in the network by various applications.

The scan process involves collecting information about each certificate, such as its subject, issuer, validity period, key length, and usage. This data helps administrators keep track of certificates' expiration dates, identify potential vulnerabilities related to weak encryption algorithms or outdated certificate versions, and ensure compliance with industry standards and best practices.

The purpose is to provide an organization with an inventory of all certificates present within their network. This inventory helps in managing and monitoring the certificates effectively, ensuring their validity, and avoiding potential security risks associated with expired or compromised certificates.

AppViewX supports certificate discovery through different types of scans as explained in the following sections:

- Network Scan
- Managed Devices Scan
- Transparency Log Scan
- Certificate Authority Scan
- Cloud Scan
- Scanning Uploaded Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- On-demand Discovery
- Scheduled Discovery

Network Scan

A network certificate discovery scan is used to identify and analyze digital certificates within a network or infrastructure. These certificates can include SSL/TLS certificates used for secure website communication, code signing certificates, client authentication certificates, and other types of digital certificates.

By performing regular network certificate discovery scans, organizations can maintain an up-to-date record of their certificates, manage them efficiently, and proactively address any security concerns or compliance issues.

Initiating a Network Discovery Scan

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Network Scan**.
   The **Discovery : Network Scan : Add Discovery** page is displayed.
2. To initiate a network certificate discovery scan, enter/select the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Network certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	Network certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter/Select the details for **initiating an on-demand network certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Note: Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled network certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, from the **Discovery From** dropdown list, select the source for the certificate discovery.
   - **Network**

Field descriptions for discovering certificates from Network

Network List	From the dropdown list, select the network(s) you want to include in the discovery. This list is populated based on the networks added to the network inventory in CERT+.
SNI Hostname(s)	To discover certificates from SNI protected websites that share the same IP and port number with another web application, enter the hostname in this field. You can also enter a comma-separated list of hostnames.

   - **IP Range**

Field descriptions for discovering certificates from IP range

Field	Description
***Start IP**	Enter the IPv4 address from which the network scan should start.
***End IP**	Enter the IPv4 address till which the network scan should run.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Ensure that the **End IP** value is greater than the **Start IP** value,
***IPs per Batch of Discovery**	Enter the number of IP addresses that should be scanned in one batch. **Note:** • A batch can include a maximum of 256 IP addresses. • Batching IP addresses for scanning in one go can be useful for throttling scan traffic.
***Scan Ports**	From the dropdown list, from the following options, select which ports have to be scanned: • **All Ports** • **Standard Ports** To get a list of the standard ports, click **Download here** from below the dropdown menu. • **Custom Ports**
Add More Ports	**Note:** This field is displayed only when **Scan Ports** = **Standard Ports**. To scan ports other than the standard ports, enter a comma-separated list of port numbers in this field. You can enter a hyphenated range of ports, as well as a comma-separated list of port ranges.
***Add Ports**	**Note:** This field is displayed only when **Scan Ports** = **Custom Ports**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter a comma-separated list of port numbers to be scanned from between 0 to 65535. You can also enter a hyphenated range of ports, as well as a comma-separated list of port ranges. For example: **444-666**, **888-999**.
Select Node to Trigger Scan From	Select the CLM node from where the discovery scan will be performed. **Note:** Select a node close to the network entered and avoid traffic through firewalls when possible.
SNI Hostname(s)	To discover certificates from SNI protected websites that share the same IP and port number with another web application, enter the hostname in this field. You can also enter a comma-separated list of hostnames.
***TLS version(s)**	From the dropdown list, select the required TLS version.
Exclusion List	From the dropdown list, select the exclusion lists that have to be used for this scan. For a network discovery scan, you can create exclusion lists that specify network sources that must be excluded from a certificate discovery scan. For instructions on viewing, creating, and managing exclusion lists, click here. **Important:** This dropdown is populated with disabled execution lists, which can be selectively enabled for a scan. Exclusion lists, once created, are automatically enabled and must be manually disabled. The disabled lists are populated in this dropdown list and can be selectively enabled.
Add	Click **Add** to add the network details entered.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The entered details are displayed in the table shown after the **Select a File** field.
Exclusion List	Same as above
Select a File	You can specifying the entries for all the above fields in a **.xlsx** or **.csv** file and upload it in this field. **Note:** To download a sample file, click **Download Sample Template**. You can fill in your details in this downloaded template. a. Click **Upload** and navigate to the location of your file. b. Click **Open**.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration in this field. The sequential execution of the batches is spaced according to the interval value entered here.
Scanning Intensity	If **Execute Batches Sequentially** is not enabled, select a scanning intensity for the discovery operation. A higher scanning intensity means a higher scanning speed and a larger network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
Skip Full Scan	Enabling this field will skip a full scan and restrict the discovery operation to sources (IP addresses and port numbers) from which certificates were discovered previously.
***Device discovery**	From the dropdown list, from the following options, select your device discovery requirement: • **Do not discover devices** Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Discover devices along with their operating system** AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed. **Note:** To discover the operating system version, AppViewX requires sudo access.
**: Mandatory fields*	

• **Subnet**

Field descriptions for discovering certificates from a subnet

Field	Description
***Network**	Enter the subnet/mask in the field. For example: **192.168.1.1/24**.
***Subnets per Batch of Discovery**	Based on the value entered, the provided subnet will be split into multiple batches for the discovery process.
***Scan Ports**	From the dropdown list, from the following options, select which ports have to be scanned: • **All Ports** • **Standard Ports** To get a list of the standard ports, click **Download here** from below the dropdown menu. • **Custom Ports**
Add More Ports	**Note:** This field is displayed only when **Scan Ports** = **Standard Ports**. To scan ports other than the standard ports, enter a comma-separated list of port numbers in this field. You can enter a hyphenated range of ports, as well as a comma-separated list of port ranges.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Add Ports**	**Note:** This field is displayed only when **Scan Ports** = **Custom Ports**. Enter a comma-separated list of port numbers to be scanned from between 0 to 65535. You can also enter a hyphenated range of ports, as well as a comma-separated list of port ranges. For example: **444-666**, **888-999**
Select Node to Trigger Scan From	Select the CLM node from where the discovery scan will be performed. **Note:** Select a node close to the network entered and avoid traffic through firewalls when possible.
SNI Hostname(s)	To discover certificates from SNI protected websites that share the same IP and port number with another web application, enter the hostname in this field. You can also enter a comma-separated list of hostnames.
***TLS version(s)**	From the dropdown list, select the required TLS version.
Exclusion List	From the dropdown list, select the exclusion lists that have to be used for this scan. For a network discovery scan, you can create exclusion lists that specify network sources that must be excluded from a certificate discovery scan. For instructions on viewing, creating, and managing exclusion lists, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: This dropdown is populated with disabled execution lists, which can be selectively enabled for a scan. Exclusion lists, once created, are automatically enabled and must be manually disabled. The disabled lists are populated in this dropdown list and can be selectively enabled.
Add	Click **Add** to add the network details entered. The entered details are displayed in the table shown after the **Select a File** field.
Exclusion List	Same as above
Select a File	You can specifying the entries for all the above fields in a **.xlsx** or **.csv** file and upload it in this field. **Note:** To download a sample file, click **Download Sample Template**. You can fill in your details in this downloaded template. a. Click **Upload** and navigate to the location of your file. b. Click **Open**.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration in this field. The sequential execution of the batches is spaced according to the interval value entered here.
Scanning Intensity	If **Execute Batches Sequentially** is not enabled, select a scanning intensity for the discovery operation. A higher scanning intensity means a higher scanning speed and a larger network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Skip Full Scan	Enabling this field will skip a full scan and restrict the discovery operation to sources (IP addresses and port numbers) from which certificates were discovered previously.
***Device discovery**	From the dropdown list, from the following options, select your device discovery requirement: • **Do not discover devices** Existing certificate scanning alone carried for the configured IPs. On completion, the batches and certificate tabs displayed. • **Discover devices along with their operating system** AppViewX scans for the device and certificates for the configured IPs. On completion, the batches, Certificates, and Devices tabs are displayed. **Note:** To discover the operating system version, AppViewX requires sudo access.
**: Mandatory fields*	

- **URL**

Field descriptions for discovering certificates from a URL

Field	Description
***URL**	Enter the HTTPS URL for discovering the associated certificate.
***Ports to Scan**	**Note:** This field is disabled if the **Scan All Ports** field is selected. Enter a comma-separated list of port numbers in this field. You can also enter a hyphenated range of ports, as well as a comma-separated list of port ranges.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Scan All Ports	**Note:** Enabling this field will disable the **Ports to Scan** field is enabled. Select the **Scan All Ports** checkbox to scan all the HTTPS-enabled ports. This is particularly useful if the number of HTTPS-enabled ports is significantly large or is unknown.
Select Node to Trigger Scan From	Select the CLM node from where the discovery scan will be performed. **Note:** Select a node close to the network entered and avoid traffic through firewalls when possible.
Add	Click **Add** to add the network details entered. The entered details are displayed in the table shown after the **Select a File** field.
Select a File	You can specifying the entries for all the above fields in a **.xlsx** or **.csv** file and upload it in this field. **Note:** To download a sample file, click **Download Sample Template**. You can fill in your details in this downloaded template. a. Click **Upload** and navigate to the location of your file. b. Click **Open**.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration in this field. The sequential execution of the batches is spaced according to the interval value entered here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Scanning Intensity	If **Execute Batches Sequentially** is not enabled, select a scanning intensity for the discovery operation. A higher scanning intensity means a higher scanning speed and a larger network load. Maximum connections from a discovery engine will be chosen based on the Scanning Intensity.
Skip Full Scan	Enabling this field will skip a full scan and restrict the discovery operation to sources (IP addresses and port numbers) from which certificates were discovered previously.

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. Configure the **After Discover** settings.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.

Managed Devices Scan

A managed devices certificate scan involves scanning and managing digital certificates on organizational devices to maintain security and prevent incidents. AppViewX's feature manages the entire certificate lifecycle on devices like ADC load balancers, servers, and firewalls, from discovery to renewal, revocation, and removal. This section details how to discover certificates, using SSL profiles and virtual servers to gather and retain certificate information.

Note: The chapter on Certificate Actions, in this guide, talks about how AppViewX manages the lifecyle of the discovered certificates.

Important: For devices with integrated gateways, discovery is performed in batches of 500 certificates.

Initiating a Managed Devices Scan

For Managed ADCs

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**. The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed ADCs**.
Devices window	A list of all the managed ADC devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

For Managed Servers

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

For Managed MDMs

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed MDMs**.
Devices window	A list of all the managed MDM devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For Managed Firewalls

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

   Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Note: Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Firewalls**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Devices window	A list of all the managed firewall devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

For Managed WAFs

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed WAFs**.
Devices window	A list of all the managed WAF devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

For Internal Devices

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Internal**.
Devices window	A list of all the managed internal devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

What's Next

After discovering certificates, you can now:

- Go to the certificate inventory to view and manage the certificates.
- Automate certificate lifecycle management by enabling:
  - Auto renewal of certificates
  - Auto regeneration of certificates
  - Auto push of certificates to endpoints
  - Alerts to notify events and status changes related to the certificates

Transparency Log Scan

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Transparency Log Scan**.
   The **Discovery : Transparency Log Scan : Add Discovery** page is displayed.
2. In the **Discover Details** section, select/enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for discovery details

Field	Description
***Discovery Run Type**	Click the check box to select the desired discovery run type. The possible types are: • **On-demand** - The user can trigger a discovery manually whenever he/she wants. • **Schedule** - By scheduling the discovery, the user can automate the process for a defined time/ frequency. **Note:** AppViewX will trigger the discovery certificates process for that instance.
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** Character limit: **2000 characters**
Note: The following fields are displayed only when **Discovery Run Type** = **Scheduled**.	
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter/select the following details:

Field descriptions for the Discover By section

Field	Description
***Discovery Log**	From the dropdown list, select the source of discovery.
***Discovery Criteria**	From the dropdown list, select the criteria that will be used for fetching certificates from the transparency log.
***Domain name**	Enter the domain name string in the ***.*** format.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.

Certificate Authority Scan

AppViewX can communicate with CA and scan certificates. To discover certificates from a CA, the CA account must be determined under the AppViewX inventory settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Important:

- Certificate discovery for CAs that include the integrated gateway functionality will be done in batches of 500 certificates.
- For the HydrantID CA, the certificate authority scan will discover only active certificates. To discover expired certificates, a rule must be created and applied at the time of triggering the certificate authority scan.

To trigger a certificate authority scan:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Certificate Authority Scan**.
   The **Discovery : Certificate Authority Scan : Add Discovery** page is displayed.
2. In the **Discover Details** section, select/enter the following details:

Field descriptions for the Discover Details section

Field	Description
***Discovery Run Type**	Click the check box to select the desired discovery run type. The possible types are: • **On-demand** - The user can trigger a discovery manually whenever he/she wants. • **Schedule** - By scheduling the discovery, the user can automate the process for a defined time/ frequency. **Note:** AppViewX will trigger the discovery certificates process for that instance.
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

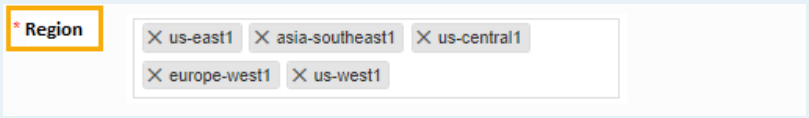
Field	Description
Note: The following fields are displayed only when **Discovery Run Type** = **Scheduled**.	
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter/select the following details:

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select the source for certificate discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Select CA**	From the dropdown list, select a CA to view its managed accounts in AppViewX for certificate discovery. **Note:** Starting version 2021.1.0, on selecting the ACM Private CA, the regions configured corresponding to the selected account are listed in the Region field. 
CA accounts table	All managed CAs will be listed in the CA accounts table, just after the **Select CA** field. Select the CAs you want to discover certificates from. The CA accounts table has the following option: • **Add as Favorites**: You can mark your frequently used CAs as favorites. • **All**: Select this to see the complete list of CAs (unfiltered). • **Selected**: Select this to list only the selected CAs. • **Unselected**: Select this to list only the unselected CAs. • **Delete**: Delete the required CA(s) from the favorites list.
Scan Type	**Scan Type** for **on-demand** discovery: • **Aggressive**: To discover all certificates from the selected CA account, select **Aggressive**. • **Optimized**: To filter and discover certificates based on a specific discovery parameter, select **Optimized**. **Scan Type** for **scheduled** discovery: • **Aggressive**: To discover all certificates from the selected CA account during every scan, select **Aggressive**. • **Optimized**: To filter and discover only the delta certificates from the selected CA (Account), during every scan, select **Optimized**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: For Microsoft CA (standalone and enterprise) configured with the integrated mode, optimized certificate discovery is not supported.
Discovery Parameters	To filter the results of the certificate authority scan, AppViewX lets you select from a list of CA-specific columns/fields, called the discovery parameters. Currently, AppViewX supports discovery parameters for the following CAs: • CSC Global • DigiCert • Entrust • HydrantID • Microsoft • Sectigo
Include Expired Certificates	**Note:** This field is displayed only for the DigiCert and HydrantID, for all scan types and discovery parameters. To include expired certificates in the discovery results, select this checkbox. By default, expired certificates are not discovered unless specified by the discovery parameters.
Include Renewed Certofoc	**Note:** This field is displayed only for the HydrantID CA, except when **Status** is one of the selected **Discovery Parameters**. To include renewed certificates in the discovery results, select this checkbox.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Discovery Parameters for CSC Global CA

Field	Description
Discovery Parameters (CSC Global)	To filter the results of the certificate authority scan, AppViewX supports the following discovery parameters for CSC Global CA: • **Certificate Status** • **Certificate Types** • **Certificate Effective Date** • **Certificate Expiration Date** To filter the discovery of CSC Global CA certificates: a. From the dropdown list, select the required discovery parameter(s). **Note:** You can select a combination of discovery parameters. However, only one from the following discovery parameters can be selected: • **Certificate Effective Date** • **Certificate Expiration Date** When one of these parameters is selected, the other one is disabled for selection. Corresponding to the discovery parameter(s) selected, a text field/ dropdown list is displayed. b. Enter/select the value(s) for the selected discovery parameter(s).
**: Mandatory fields*	

Discovery Parameters for DigiCert CA

Field	Description
Discovery Parameters (DigiCert CA)	To filter the results of the certificate authority scan, AppViewX supports the following discovery parameters for DigiCert CA: • **None** • **Product Name** (multiple values can be selected) • **Common Name** • **Order ID** (multiple values can be selected) • **Certificate ID** • **Status** • **Domain Name**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Organization ID** (multiple values can be selected) • **Expires On** • **Certificate Created On** (to discover certificates created within the selected date range; the date range must not exceed two years) • **Expiring Before** (to discover certificates expiring before the selected date; discovery does not include certificates expiring on the selected date) • **Expiring After** (to discover certificates expiring after the selected date; discovery does not include certificates expiring on the selected date) To filter the discovery of DigiCert CA certificates: a. From the dropdown list, select the required discovery parameter. Corresponding to the discovery parameter selected, a text field/ dropdown list is displayed. b. Enter/select the value for the selected discovery parameter.
**: Mandatory fields*	

Discovery Parameters for Entrust CA

Field	Description
Discovery Parameters (Entrust CA)	To filter the results of the certificate authority scan, AppViewX supports the following discovery parameters for Entrust CA: **certificate status** and **certificate type** To filter the outcome of the certificate authority discovery for Entrust CA, from the **Discovery Parameters** dropdown list, select the parameter(s). **Important:** The discovery parameters specified in the subsequent fields will take precedence over the **Associate Rule** specified in the **Discovery Rules** section. **Important:** If the certificates discovered basis the discovery parameters have associated root and/or intermediate certificates, those certificates will also be included in the results, irrespective of their type and status.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Status	This field is displayed only when **Select CA** = **Entrust** and **Discovery Parameters** = **Certificate Status**. To filter the certificate authority discovery for Entrust CA based on the certificate status, from this dropdown menu, select the required status value(s). **Important:** When **Certificate Status** = **Declined, Pending**, the discovery will return no certificates, since in both these events (when a certificate enrollment is declined or is pending), the end entity certificate has not been created.
Certificate Type	This field is displayed only when **Select CA** = **Entrust** and **Discovery Parameters** = **Certificate Types**. To filter the certificate authority discovery for Entrust CA based on the certificate type, from this dropdown menu, select the required type(s).
**: Mandatory fields*	

Discovery Parameters for HydrantID CA

Field	Description
Discovery Parameters (HydrantID CA)	To filter the results of the certificate authority scan, AppViewX supports the following discovery parameters for HydrantID CA: • **Certificate Types** • **Created From** • **Updated From** • **Not Before** • **Not After** • **Common Name** • **Serial Number** • **Status** • **Owner** • **Account** • **Organization** From the dropdown list, select the required discovery parameter.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Types**	This field is displayed when **Certificate Types** is one of the selected **Discovery Parameters**. To filter the certificate authority discovery for HydrantID CA based on the certificate types, from this dropdown menu, select a certificate type based on the required certificate characteristics and use cases.
***Created From**	This field is displayed when **Created From** is one of the selected **Discovery Parameters**. To filter discovery results based on the certificates' initial creation date, use the (calendar) widget to select the required date. The discovery results are then filtered to include only those certificates that were created between the selected date and the current date. **Example**: If the selected date is 2022-04-07, then the discovery results will include only those certificates that were created between 2022-04-07 and the current date. **Important:** The maximum allowed date range is **three** years from the current date.
***Updated From**	This field is displayed when **Updated From** is one of the selected **Discovery Parameters**. To filter discovery results based on the most recent certificate update date, use the (calendar) widget to select the required date. The discovery results are then filtered to include only those certificates that were updated between the selected date and the current date. **Example**: If the selected date is 2022-04-07, then the discovery results will include only those certificates that were updated between 2022-04-07 and the current date.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: The maximum allowed date range is **three** years from the current date.
Not Before	This field is displayed when **Not Before** is one of the selected **Discovery Parameters**. To filter discover results based on when a certificate's validity period begins, use the (calendar) widget to select the required date. The discovery results are filtered to include only those certificates that become valid after the selected date, which means the certificates are **not** valid **before** the selected date.
Not After	This field is displayed when **Not After** is one of the selected **Discovery Parameters**. To filter discovery results based on when a certificate's validity period ends, use the (calendar) widget to select the required date. The discovery results are filtered to include only those certificates that are **not** valid **after** the selected date.
***Common Name**	This field is displayed when **Common Name** is one of the selected **Discovery Parameters**. To filter certificates based on a specific common name, enter the required common name in this field.
***Serial Number**	This field is displayed when **Serial Number** is one of the selected **Discovery Paramters**. To filter certificates based on the unique identifier assigned to them by the issuing Certificate Authority (CA), enter the required serial number in this field.
***Status**	This field is displayed when **Status** is one the selected **Discovery Parameters**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To filter certificates based on their current status, from the dropdown list, select the required status value.
***Owner**	This field is displayed when **Owner** is one of the selected **Discovery Parameters**. To filter discovery results based on the designated owner responsible for managing the certificates, enter the required owner name in this field.
***Account**	This field is displayed when **Account** is one of the selected **Discovery Parameters**. To filter discovery results based on the user account associated with a certificate, enter the required account name in this field.
***Organization**	This field is displayed when **Organization** is one of the selected **Discovery Parameters**. To filter discovery results based on the organization, enter the required organization name in this field. An organization is the entity to which a certificate is issued and which is used to validate the ownership and authenticity of the certificate.
**: Mandatory fields*	

Discovery Parameters for Microsoft CA

Field	Description
Discovery Parameters (Microsoft CA)	To filter the results of the certificate authority scan, AppViewX supports the following discovery parameters for Microsoft CA: • **Requester Name** • **Certificate Template** • **Common Name** • **Certificate Effective Date** • **Certificate Expiration Date** • **Time Range**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To filter the discovery of Microsoft CA certificates: a. From the dropdown list, select the required discovery parameter(s). **Note:** You can select a combination of discovery parameters. However, only one from the following discovery parameters can be selected: • **Certificate Effective Date** • **Certificate Expiration Date** • **Time Range** When one of these three parameters is selected, the other two are disabled for selection. Corresponding to the discovery parameter(s) selected, a text field/ dropdown list is displayed. b. Enter/select the value(s) for the selected discovery parameter(s).
**: Mandatory fields*	

Discovery Parameters for Sectigo CA

Field	Description
Discovery Parameters (Sectigo CA)	To filter the results of the certificate authority scan, AppViewX supports the following discovery parameters for Sectigo CA: • **Start Date** • **End Date** Using these parameters, you can specify a date range to discover only those certificates that were issued between the specified start and end dates.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**. **Note:** If the discovered certificate already exists in the inventory, its objects will be moved with the same status.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.

Note:

- For **EJBCA**

  The revoked certificates are not discovered. On discovery, the end certificates are discovered based on the days configured in the CA settings, the expired certificates are always discovered. The expiry days calculate from 0 - given value, for example, 0 -1500. On discovery, all the root and intermediate certificates that expire before 100 years will be discovered along with the end certificates by default. The discovered certificate count cannot be validated against the certificates present in the CA.

- For **Hydrant ID CA**

  Starting v2024.0.2.0, the triggered discovery instance will also fetch the expiry email addresses specified for the Hydrant ID CA certificates.

  For existing certificates that are not yet updated for this detail, triggering a new discovery instance will fetch the details and the discovery details will be automatically updated when the inventory status is moved to **Managed** state.

Cloud Scan

A cloud discovery scan lets you identify certificates in use within your cloud environment. The discovery is filtered based on specific cloud environments and identifies certificates irrespective of the issuing certificate authority.

Initiating a Cloud Discovery Scan for Azure

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	• **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that constitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Once the certificates are discovered, you can view them in the certificate inventory.

To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

What's Next?

To automate certificate lifecycle management for certificates discovered from your Azure account:

- Enable auto regeneration of certificates.
- Enable auto push of certificates to endpoints. To do this, add an application connector to push the certificate to an AWS device and select the **Push Automatically** checkbox.
- Set alerts to be notified of all events and statuses of the certificates.

Initiating a Cloud Discovery Scan for AWS

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Note: Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)
***Select Account View**	**Note:** This field is displayed only when you've selected **Account type** = **Cross account sign-in**. From the given options, select one to specify if the discovery will be performed for the master account or for the child accounts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Select Filter Type**	**Note:** This field is enabled when: • • **Account type** = **Stand-alone account sign-in** • **Account type** = **Cross account sign-in** AND **Select Account View** = **Child Account**. From the following options, select one to specify how the discovery results should be filtered: • **Account View** • **Service View**
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are listed in the certificate inventory.

What's Next?

To automate certificate lifecycle management for certificates discovered from your AWS account:

- Enable auto regeneration of certificates.
- Enable auto push of certificates to endpoints. To do this, add an application connector to push the certificate to an AWS device and select the **Push Automatically** checkbox.
- Set alerts to be notified of all events and statuses of the certificates.

Initiating a Cloud Discovery Scan for GCP

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, from the following options, select GCP.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Discovery Scope	Select the GCP environment scope (range/boundary) within which the certificate discovery process will operate. • **GCP Settings** GCP settings are configurable parameters that define the behavior of the resources within a project. • **GCP Projects** GCP projects are logical containers that constitute the GCP resources, identified based on a specific requirement.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **GCP Projects**. To filter discovery results based on the services under each project mapped to a setting, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a project that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.

Scanning Uploaded Certificates

You can upload individual certificates or you can zip a group of certificates and then add them. For Windows-related servers and CA communication, an agent should be installed and configured in AppViewX.

To scan the uploaded certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Upload**.
   The **Discovery : Upload : Add Discovery** page is displayed.
2. In the **Discover Details** section, select/enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Discover Details section

Field	Description
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** Character limit: **2000 characters** .

3. In the **Discover By** section, enter the following details:

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select the source of the discovery.
***Choose File**	You can upload a certificate file in one of the following formats: **.zip**, **.tar**, **tar.gz**, **.crt**, **.cer**, **.der**, **.p7b**, **.p7c**, **.pem**, **.pfs**, **.jks**, **.p12**. To upload a certificate file: a. Click **Upload** and navigate to the location of the required certificate file. b. Select the file and click **Open**.
***File Password**	If the certificate file uploaded in **Choose File** is password-protected, in this field, enter the password for accessing the file.
Comments	Enter any additional remarks or details related to the process.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery.

On-demand Discovery

On-demand discovery is a discovery process execution type that is triggered immediately (as opposed to a scheduled discovery that is triggered according to a predefined schedule, and not necessarily immediately).

There are two ways you can trigger an on-demand discovery, as explained in the following sections.

On-demand Discovery: Method 1

This method is useful when you know the type of discovery process you want to trigger, from the following types:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Network scan
- Managed devices scan
- Transparency log scan
- Certificate authority scan
- Cloud scan

For each of these scan types, the form fields described in the respective sections explain the option that lets you specify whether the discovery will be on-demand or scheduled.

Click a scan type from the list above for instructions on how you can select on-demand discovery for that type.

On-demand Discovery: Method 2

The difference between method 1 and method 2 is that the **Discovery From** dropdown list for method 2 lists the sources for all discovery types.

To trigger an on-demand discovery:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**. The **Discovery Status : On-demand** page is displayed. .
2. To create a new on-demand discovery distance:

   If this is the first on demand discovery instance, click Discover Now from the center of the page.

   OR

   Click + Create Discovery .
3. In the **Discover Details** section, enter the following details:

Field descriptions for the Discover Details section

Field	Description
***Discovery Run Type**	Select **On-demand**.
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Character limit: **2000 characters**
**: Mandatory fields*	

4. In the **Discover By** section, from the **Discovery From** dropdown list, select the source of the discovery.
   Based on your selection in this field, the rest of the fields will be displayed. For instructions on specifying the rest of the details:

Field descriptions for the Discover By section

Selection	Refer for further instructions
• **IP Range** • **Subnet** • **URL**	Network Scan
• **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**	Managed devices scan
CtLogs	Transparency Log Scan
Certificate Authorities	Certificate Authority Scan
Cloud	Cloud Scan
Upload	Scanning Uploaded Certificates
**: Mandatory fields*	

5. In the **Discovery Rules** section, select the associate rule from dropdown list.
6. In the **After Discover** section, select the required options.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select the required options as required. The available options are, • **Do not move** • **Managed** • **Monitored**.
Use Access Control Rule	Enable the checkbox to apply rule. **Note:** This dield is enabled when **Move Certificate to Inventory with Status** = **Managed** or **Monitored**.
Certificate Group	Select the required certificate group. Discovered certificates will be associated with the provided certificate group.
**: Mandatory fields*	

7. In the **Discovery Notifications** section, select the notification field as required.

Field descriptions for the Discovery Notifications section

Field	Description
Subscribe for discovery status notifications	Select the checkbox for the notification.
Who should be notified ?	• **Notify User**: Send notification to the user configuring/modifying the discovery. • **Notify User-Group**: Send notification to all the users in the triggering User's User Group(s).
**: Mandatory fields*	

Scheduled Discovery

Scheduled discovery is a discovery process execution type that lets you trigger a discovery process one/multiple times according to a predefined schedule.

There are two ways you can schedule a discovery process, as explained in the following sections.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Scheduled Discovery: Method 1

This method is useful when you know the type of discovery process you want to trigger, from the following types:

- Network scan
- Managed devices scan
- Transparency log scan
- Certificate authority scan
- Cloud scan

For each of these scan types, the form fields described in the respective sections explain the option that lets you specify whether the discovery will be on-demand or scheduled.

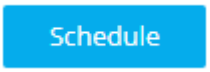
Click a scan type from the list above for instructions on how you can select on demand discovery for that type.

Scheduled Discovery: Method 2

The difference between method 1 and method 2 is that the **Discovery From** dropdown list for method 2 lists the sources for all discovery types.

To trigger a scheduled discovery:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** >**Scheduled**.
   The **Discovery Status : Scheduled** page is displayed. .
2. To create a new on demand discovery distance:

   If this is the first scheduled discovery instance, click 

from the center of the page.

   OR

   Click

.
3. In the **Discover Details** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Discover Details section

Field	Description
***Discovery Run Type**	Select **Scheduled**.
Discovery Instance Name	Enter the name of the discovery instance.
Description	Enter the required details in this field. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

4. In the **Discover By** section, from the **Discovery From** dropdown list, select the source of the discovery.
   Based on your selection in this field, the rest of the fields will be displayed. For instructions on specifying the rest of the details:

Field descriptions for the Discover By section

Selection	Refer for further instructions
• **IP Range** • **Subnet** • **URL**	Network Scan
• **Managed ADCs** • **Managed Servers** • **Managed MDMs** • **Managed Firewalls** • **Managed WAFs** • **Internal**	Managed devices scan
CtLogs	Transparency Log Scan
Certificate Authorities	Certificate Authority Scan
Cloud	Cloud Scan
Upload	Scanning Uploaded Certificates

Discovery Status

The discovery status section gives a summary of the on-demand and scheduled discoveries triggered. In addition to this, the discovered certificates can be filtered for their status, exclusion in the discovery list, and so on.

- Viewing Discovery Summary
- Excluding Unmanaged Certificate
- Updating Discovered Certificates Status
- Executing a Scheduled Discovery Scan Before Schedule
- Exporting Details of Discovered Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Aborting Certificate Discovery
- Delta Discovery
- Viewing the Scan Status of a Discovery Instance

Viewing Discovery Summary

Certificate discovery Summary is displayed as a dashboard that provides a high-level overview of a discovery instance's results. It presents a set of statistics and visual widgets that highlight certificate distribution across various categories.

To view the discovery summary:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous and active discovery instances triggered are listed here.

   Note: When a scheduled discovery scan is triggered, it is also listed in the on-demand inventory.

2. To view the summary of a discovery instance, click the discovery instance's **Name**.
   By default, the summary details of the selected discovery instance are displayed.

   The summary details are displayed in two parts:
   - Certificate Discovery Summary
   - Certificate Summary widgets

   Certificate Discovery Summary

Field	Description
Total Certificates	Total number of certificates currently associated with this discovery instance. This includes all certificates discovered during the scan, including any that were previously known or re-identified.
Discovered Certificates	Number of certificates discovered in the most recent execution of this discovery instance
Password Protected Certificates	Number of certificates discovered during the scan that are stored in password-protected file formats

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Encrypted Private Keys	Number of private keys found during the discovery scan that are encrypted

Certificate Summary widgets

Field	Description
Certificate Summary	This widget gives a quick snapshot of the overall certificate landscape, showing the number of newly discovered certificates and the proportion that are actively managed or monitored.
Certificate Distribution by Category	This widget shows the number of certificates across certificate categories. Understanding this distribution helps you identify the primary uses of certificates in your environment and potential areas of focus for management and security policies.
Certificate Distribution by Issuer	This widget visualizes certificate distribution based on the issuing authority. Knowing which entities issued your certificate is crucial for trust management and for understanding your dependencies on different Certificate Authorities (CAs).
Certificate Status Report	This widget provides a breakdown of certificates based on their expiration status (certificates nearing expiry, already expired, and revoked). This data is critical for proactive certificate management, enabling timely renewal and preventing service disruptions or security vulnerabilities. The number of revoked certificates is also an indicator of potential security incidents or policy enforcement actions.
Certificates by Key Algorithm Strength	This widget shows certificate distrbution based on the cryptographic strength of certificate key algorithms, helping you assess the overall security posture of your certificate landscape. A high number of certificates with low or medium strength key algorithms might indicate potential vulnerabilities and the need for

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	upgrades to stronger algorithms. Ideally, you want the majority of your certificates to fall into the **high** strength category.
Certificates by Hash Algorithm Strength	This widget shows certificate distribution based on the strength of their hash algorithms. This assessment helps you prioritize migration of certificates using weaker hash algorithms to stronger, more secure ones.
Certificates Usage by Type	This widget shows the distribution of certificate usage across all supported certificate types. The widget displays certificates grouped by type (e.g., DV, OV, EV, Wildcard, SAN, Self-signed, etc.). Since a single certificate can belong to multiple categories (e.g., an EV certificate can also be a Wildcard or SAN certificate), it is counted in each applicable type. As a result, the sum of all certificate types shown here may exceed the actual number of unique certificates discovered. This design helps you understand certificate usage patterns across categories, even when overlaps occur.
Vendor Type Distribution	This widget displays certificate distribution based on the vendors of the devices or servers where the certificates were discovered. When populated, this widget would help you understand your reliance on different device/server vendors. This information can be valuable for vendor management, cost analysis, and ensuring diversity or consolidation of your application infrastructure providers based on your organisational policies. It can also help in identifying potential single points of failure related to a specific vendor.
Certificates with Trusted vs Untrusted CA Status	This widget displays certificate distribution based on whether they are issued by trusted or untrusted certificate authorities (CAs). This widget is crucial for assessing the trustworthiness and security of your certificate ecosystem. Ideally, you want the vast majority of your certificates to be issued by trusted CAs. A high number of untrusted certificates can indicate potential security risks, misconfigurations, or the use of self-signed certificates where CA-

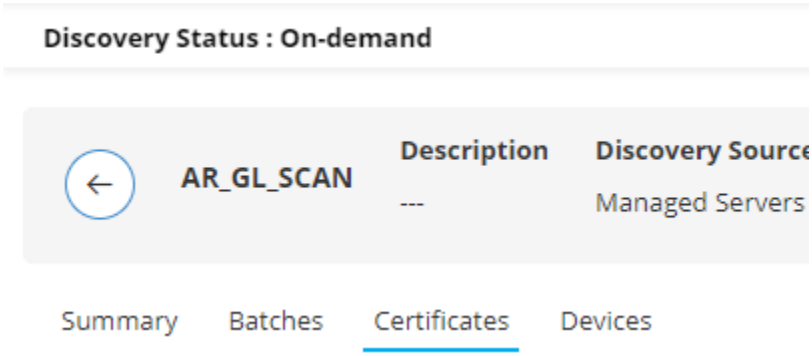
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	signed ones are recommended. Investigating and addressing untrusted certificates is vital for maintaining a secure environment.
PQC Compliance Certificates	This widget displays certificate distribution based on their compliance with post-quantum cryptography (PQC) standards. As quantum computing technology advances, the cryptographic algorithms we rely on today may become vulnerable. This widget helps you understand your organisation's readiness for the post-quantum era. A high number of non-compliant certificates signifies a potential future security risk, and planning for migration to PQC-compliant algorithms will be essential in the long term. Currently, with all certificates marked as non-compliant, it highlights an area to monitor and prepare for as PQC standards and implementations evolve.
MTLS Adoption Report	This widget displays the number of endpoints (IP:Port combinations) with Mutual TLS (mTLS) enabled, as detected during network-based discovery. Mutual TLS ensures both the client and the server authenticate each other using certificates, adding a stronger layer of security over standard TLS.

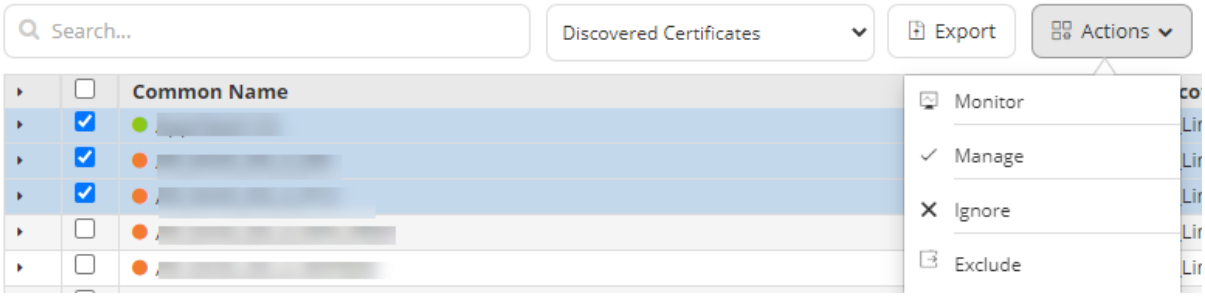
Excluding Unmanaged Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous discovery instances triggered are listed here.
2. To view the details of a discovery operation, click the **Name**.
   The **Discovery Status : On-demand** page is updated to show the details of the discovery instance.
3. To view the certificates discovered by this discovery instance, click **Certificates**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. To exclude a certificate, from the list of certificates displayed, click the checkbox corresponding to the required certificate.
   You can select multiple such certificates.
5. From the **Actions** menu, click **Exclude**.



6. From the **Exclude** confirmation dialog box, click **Yes**.

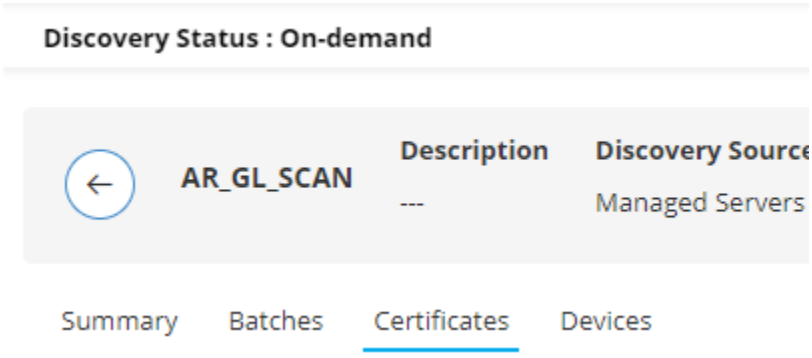
> **Note:** Excluded certificates will be removed from the current discovery instance and will be added to the **Excluded from discovery** inventory.

Updating Discovered Certificates Status

To set the discovered certificate status to **Monitor/Manage/Ignore/Exclude**:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous discovery instances triggered are listed here.
2. To view the details of a discovery operation, click the **Name**.
   The **Discovery Status : On-demand** page is updated to show the details of the discovery instance.
3. To view the certificates discovered by this discovery instance, click **Certificates**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. From **Name**, select the checkbox for the certificate that you want to filter.
5. From the **Actions** menu, select the new certificate status from the following options:
   - **Monitor**
   - **Manage**
   - **Ignore**
   - **Exclude**
6. Click **Yes**.

Bulk Updating Discovered Certificates Status

To bulk update the status of the discovered certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous discovery instances triggered are listed here.
2. Select the checkbox against the column name **Common name**.
   The option to **Select All () Certificates present in Discovery Inventory**.
3. Click **Select All () Certificates present in Discovery Inventory**.
   All discovered certificates in the inventory are selected.
4. From the **Actions** menu, select the new certificate status from the following options:
   - **Monitor**
   - **Manage**
   - **Ignore**
   - **Exclude**
5. To view details of the bulk certificate status update operation, go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Certificate Logs**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:
- Root and intermediate certificates can be moved only to the managed status.
- Inventoried certificates cannot be moved to the monitored/managed status.

The tooltip text for the corresponding entry of this operation in the certificate log includes the complete details of the operation.

Executing a Scheduled Discovery Scan Before Schedule

In addition to running at their configured intervals, scheduled discovery scans can now be triggered manually, ahead of their predefined schedule. This capability is particularly useful in time-sensitive scenarios where the latest certificate is required for purposes such as troubleshooting or compliance.

Important: This feature is RBAC-controlled, which means only authorized users will be able to see the corresponding menu option and trigger a scheduled discovery before time.

To execute a scheduled discovery scan manually, ahead of its schedule:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **Scheduled**.
   The **Discovery Status : Scheduled** page is displayed, listing all existing scheduled discovery instances.
2. To manually trigger a scheduled discovery instance, select the checkbox corresponding to that discovery instance.
3. From the **Actions** dropdown menu, select **Run now**.
   The message **Discovery execution has been triggered successfully** is displayed and the active discovery instance is moved into the on-demand discovery instances inventory.

Note: This does not impact the scheduled discoveries; they will be triggered as per the configured schedule.

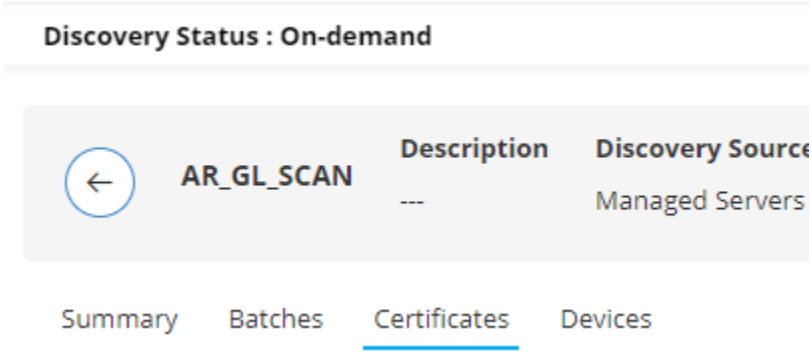
Exporting Details of Discovered Certificates

AppViewX lets you export all/selected details of the certificates discovered by a discovery instance. You can export the details in the XLS or CSV format.

To export the details of discovered certificates:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** >**On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous discovery instances triggered are listed here.
2. To view the details of a discovery operation, click the **Name**.
   The **Discovery Status : On-demand** page is updated to show the details of the discovery instance.
3. To view the certificates discovered by this discovery instance, click **Certificates**.



4. From **Name**, select the checkbox for the certificate of which you want to export the details.
5. Click **Export**.
   The **Export** dialog box is displayed.
6. In the **Export** dialog box:
   a. Under **Options**, select if you want to export all the details or only those shown in the columns currently displayed.
   b. Under **Format**, select the format for the exported file.
7. Click **Export**.
   A **.csv**/**.xls** file (as selected) is downloaded to your system.

Aborting Certificate Discovery

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous discovery instances triggered are listed here.
2. From **Name**, select the checkbox for the discovery instance you want to abort.
3. From the **Actions** dropdown menu, select **Abort**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Delta Discovery

Delta Discovery of certificates involves discovering only those certificates that have been pushed to the device, modified, or removed from the inventory since the last config sync. It is available and limited to Fetch Config and Midnight Sync for

- IBM MQ server (Linux)
- Generic Linux devices
- Apache Linux Server

When Fetch Config is carried out for the first time, it will pull all the certificates from the server. However, every Fetch config after that will only pull the delta certificates, that is the certificates added to the device since the last sync. Behavior for on-demand discovery and Config sync after Save/Edit to the device remains the same as before, that is all the certificates will be discovered.

Viewing the Scan Status of a Discovery Instance

CERT+ discovery feature has been enhanced to include endpoint checks for mTLS enforcement and supported cipher suites. You can enable these checks under **Discovery Configuration** > **Report Settings**, as explained here.

When enabled, these settings capture detailed endpoint-level data for each network scan discovery instance and are displayed as the scan status.

To access the scan status:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **On Demand**.
   The **Discovery Status : On-demand** page is displayed. Results of all previous and active discovery instances triggered are listed here.

   Note: When a scheduled discovery scan is triggered, it is also listed in the on-demand inventory.

2. To view the summary of a discovery instance, click the discovery instance's **Name**.
   The summary details of the selected discovery instance are displayed.
3. To view the scan status for the selected instance, click **Scan Status**.
   The page is updated to display the scan status details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Scan Status Toolbar

Field	Description
Search	Use the search field to execute a free text seach across the **IP**, **Port**, and **Status** fields in the scan status details.
	To narrow down search results based on specific criteria, click and, in the **Advanced Search** dialog box, enter the required details.
Export	To export the scan results, click **Export** and select the required format from the following options: • CSV • XLS
	Use the pagination control dropdown to select the number of records that will be displayed per page of the scan status details. You can select to display 25, 50, 75, or 100 records per page.
	Use the pagination navigation buttons to move between pages in the scan status details.
	Use the **Refresh** button to reload the scan status detail to display the up-to-date records.

Scan Status Details

Field	Description
IP	IP addresses of all the endpoints discovered by this discovery instance
Port	Port number scanned
Status	Status of the checks for mTLS, Cipher Suite enablement, and data fetch

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This column displays one of the following values: • **Success** (when both mTLS and Cipher Suite data is fetched successfully) • **Failed** (when an internal error occurs or the data fetch fails) • **Disabled** (when both mTLS and Check and Cipher Suite Reports are not enabled in the Report Settings) To view the scan status summary, click .
MTLS	mTLS enforcement status for the corresponding endpoint This column displays one of the following values: • **Enabled** (mTLS is enforced and enabled on the endpoint) • **Disabled** (mTLS is enforced and disabled on the endpoint) • **NA** (mTLS is not enforced on the endpoint)
Ciphers	List of ciphers enabled in the endpoint

Discovery Exclusions

• Certificate Exclusions

Certificate Exclusions

This feature helps you if you do not want a certificate or a list of certificates to be discovered. You can exclude those certificates from getting discovered.

To exclude certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Excluded Certificates**.
   The **Excluded Certificates** page is displayed.
2. To view the details of a discovery operation, click the **Common Name**.
3. To view the certificates discovered by this discovery instance, click **Certificates**.
4. From **Common Name**, select the checkbox for the certificates that you want to exclude.
5. From the **Exclude** confirmation dialog box, click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Discovery Configuration

- Network Exclusions
- Port Exclusions
- Network Inventory
- Discovery Configuration Settings

Network Exclusions

For a network scan, AppViewX lets you create a list of network sources that have to be excluded from the scans. This list is called an exclusion list and it is made of IP addresses and/or subnets that have to be excluded from a network discovery scan. Exclusion lists are different from rules; while rules let you exclude IP addresses after a discovery operation is completed, an exclusion list will do the same thing but before the discovery operation is triggered.

Creating an Exclusion List

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Networks**.
   The **Excluded Networks** page is displayed.
2. Click **+ Create**.
   The **Add** page is displayed.
3. Enter/Select the exclusion list details.

   Important: Maximum of 5000 exclusion list is allowed.

   Field descriptions for the exclusion list details

Field	Description
***Excluded IP Name**	Enter a name for the exclusion list. **Important:** This field does not support special characters.
Description	Add a short description with the reason to be excluded.

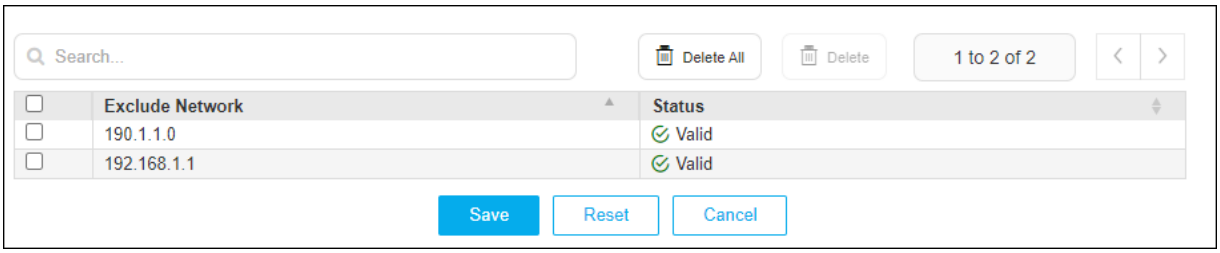
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Network Setting	Select a network setting to enforce this excluded network across all associated networks. The available options are: • **All** • **Custom**.
***Select Settings**	Select the network settings that applies to this entry. **Note:** This field appears when **Network Setting** = **Custom**.
***Exclusion By**	From the dropdown list, from the following options, select the source of the exclusion list: • **Custom**: Lets you enter a list of the IP addresses and/or subnets to be excluded from the network scan • **Upload**: Lets you upload a file that has the IP addresses and/or subnets to be excluded from the network scan Acceptable file formats: **.xlsx**, **.xls**, **.csv** **Important:** To view a sample exclusion list file: a. From this dropdown list, select **Upload**. The **Upload File** field is displayed. b. From below the **Upload File** field, click **Download Sample Template**. The sample template will be downloaded to your system.
***Exclude List**	This field is displayed if **Exclusion By** = **Custom**. Enter a valid IP address, subnet, IP range, or a combination of these network sources for exclusion from all network discovery scan(s). Listed below are examples of valid values: • Sample value for IP address: **192.168.1.1** • Sample value for subnet: **192.168.1.1/24** • Sample value for a range of IP addresses: **192.168.1.1 – 192.168.1.10**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Browse**	This field is displayed if **Exclusion By** = **Upload**. To upload a **.xlsx/.xls/.csv** file that has the exclusion list: a. Click **Upload**. b. Navigate to the location of the file. c. Select the required file. d. Click **Open**. **Important:** To view a sample exclusion list file: a. From below the **Upload File** field, click **Download Sample Template**. The sample template will be downloaded to your system.
**: Mandatory fields*	

4. Click **Add.**
   The table below the fields is populated with entries from the **Exclusion List**/file uploaded with the exclusion list.



5. Click **Save.**
   If an excluded IP address/subnet was previously discovered and is already part of the inventory, the current discovery operation will not change that. If required, you can manually delete the corresponding certificates from the inventory.

Disabling an Exclusion List

By default, exclusion lists are enabled as soon as they are created. Which means that when a network discovery operation is triggered, the results will exclude all the network sources that are a part of the exclusion lists. You can choose to disable an execution list so that it is not considered for the subsequent network discovery scans.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Additionally, you can enable selected disabled exclusion lists for a specific scan at the time of configuring the scan, by selecting the required list(s) from the **Exclusion Lists** dropdown list.

To disable an exclusion list:

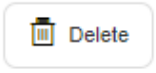
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Networks**.
   The **Excluded Networks** page is displayed.
2. From the exclusion list inventory, under **Status**, move the radio button to left that you want to disable.
   The confirmation dialog box appears as **Excluded Netwrok Successfully Disabled**.

Enabling an Exclusion List

To enable an exclusion list after it has been disabled:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Networks**.
   The **Excluded Networks** page is displayed.
2. From the exclusion list inventory, under **Status**, move the radio button to right that you want to enable.
   The confirmation dialog box appears as **Excluded Netwrok Successfully Enabled**.

Deleting an Execution List

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Networks**.
   The **Excluded Networks** page is displayed.
2. From the exclusion list inventory, under **Exclude Network**, select the checkbox(es) corresponding to the exclusion list(s) you want to delete.
3. From the menu bar, click 

.
4. From the confirmation dialog box, click **Submit**.
   The selected exclusion list(s) are deleted.

Port Exclusions

For a network scan, AppViewX lets you create a list of port sources that have to be excluded from the scans. This list is called an exclusion list and it is made of IP addresses and/or subnets that have to be excluded from a network discovery scan. Exclusion lists are different from rules; while rules let you

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

exclude port addresses after a discovery operation is completed, an exclusion list will do the same thing but before the discovery operation is triggered.

Creating an Exclusion List

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Ports**.
   The **Excluded Ports** page is displayed.
2. Click **+ Create**.
   The **Add** page is displayed.
3. Enter/Select the exclusion list details.

> **Important:** Maximum of 5000 exclusion list is allowed.

Field descriptions for the exclusion list details

Field	Description
***Excluded Ports Name**	Enter a name for the exclusion list. **Important:** This field does not support special characters.
Description	Add a short description with the reason to be excluded.
Network Setting	Select a network setting to enforce this excluded network across all associated networks. The available options are: • **All** • **Custom**.
***Select Settings**	Select the network settings that applies to this entry. **Note:** This field appears when **Network Setting** = **Custom**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Exclusion By**	From the dropdown list, from the following options, select the source of the exclusion list: • **Custom**: Lets you enter a list of the Port addresses and/or subnets to be excluded from the network scan. • **Upload**: Lets you upload a file that has the IP addresses and/or subnets to be excluded from the network scan Acceptable file formats: **.xlsx**, **.xls**, **.csv** **Important:** To view a sample exclusion list file: a. From this dropdown list, select **Upload**. The **Upload File** field is displayed. b. From below the **Upload File** field, click **Download Sample Template**. The sample template will be downloaded to your system.
***Excluded Ports**	This field is displayed if **Exclusion By** = **Custom**. Enter a valid port numbers between 1 to 65535.
***Browse**	This field is displayed if **Exclusion By** = **Upload**. To upload a **.xlsx/.xls/.csv** file that has the exclusion list: a. Click **Upload**. b. Navigate to the location of the file. c. Select the required file. d. Click **Open**. **Important:** To view a sample exclusion list file: a. From below the **Upload File** field, click **Download Sample Template**. The sample template will be downloaded to your system.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Click **Add.**
   The table below the fields is populated with entries from the **Exclusion List**/file uploaded with the exclusion list.
5. Click **Save.**

Disabling an Exclusion List

By default, exclusion lists are enabled as soon as they are created. Which means that when a network discovery operation is triggered, the results will exclude all the network sources that are a part of the exclusion lists. You can choose to disable an execution list so that it is not considered for the subsequent network discovery scans.

Additionally, you can enable selected disabled exclusion lists for a specific scan at the time of configuring the scan, by selecting the required list(s) from the **Exclusion Lists** dropdown list.

To disable an exclusion list:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Ports**.
   The **Excluded Ports** page is displayed.
2. From the exclusion list inventory, under **Status**, move the radio button to left that you want to disable.
   The confirmation dialog box appears as **Excluded Port Successfully Disabled**.

Enabling an Exclusion List

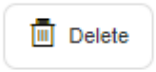
To enable an exclusion list after it has been disabled:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Ports**.
   The **Excluded Ports** page is displayed.
2. From the exclusion list inventory, under **Status**, move the radio button to right that you want to Enable.
   The confirmation dialog box appears as **Excluded Port Successfully Enabled**.

Deleting an Execution List

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Excluded Ports**.
   The **Excluded Ports** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. From the exclusion list inventory, under **Excluded Ports**, select the checkbox(es) corresponding to the exclusion list(s) you want to delete.
3. From the menu bar, click 

.
4. From the confirmation dialog box, click **Submit**.
   The selected exclusion list(s) are deleted.

> **Note:** Default ports cannot be deleted.

Network Inventory

The **Network Inventory** feature defines where certificate discovery should occur by listing specific IP addresses for scanning. It supports manual entry and bulk upload, with tagging options like datacenter or application name. This focused approach avoids scanning irrelevant areas, improves efficiency, and ensures consistent, repeatable discovery across key network segments like DMZs and app layers.

Adding Networks to the Network Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Network Inventory**.
   The **Discovery Configuration :: Network Inventory** page is displayed.
2. Click **+ Create**.
   The **Discovery Configuration :: Network Inventory > Add** page is displayed.
3. Enter/Select the **Basic Details** of the network you want to add to the inventory.

Field descriptions for the Basic Details

Field	Description
***Name**	Enter a name for the network. **Important:** This field does not support special characters.
Description	Add additional details about the network entry.
***Network Settings**	Select a network setting that applies to this entry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Network Input By**	From the dropdown list, from the following options, select the source of the network entry list: • **Custom**: Lets you enter a list of the port addresses and/or subnets to be excluded from the network scan. • **Upload**: Lets you upload a file that has the IP addresses and/or subnets to be listed in the network inventory. Acceptable file formats: **.xlsx**, **.xls**, **.csv** **Important:** To view a sample network list file: a. From the **Network Input By** dropdown list, select **Upload**. The **Upload File** field is displayed. b. From below the **Upload File** field, click **Download Sample Template**. The sample template will be downloaded to your system.
***Network List**	For **Network Input By** = **Custom** Enter the IP addresses, IP address ranges, or subnets that have to be listed in the network inventory. Separate multiple entries with commas or a new line. For **Network Input By** = **Upload** To upload a **.xlsx/.xls/.csv** file that has the netwprk list: a. Click **Upload**. b. Navigate to the location of the file. c. Select the required file. d. Click **Open**.
**: Mandatory fields*	

4. Click **Add**.
   The network details are listed in the table below the **Add** button.
5. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Disabling Networks Listed in the Network Inventory

You can disable a network listed in the network inventory to exclude it from a discovery instance. This helps avoid scanning irrelevant or restricted networks, reduce duplicates, or optimize performance. The disabling is temporary and the networks can be re-enabled when needed.

Networks can be disabled even if they are included in scheduled certificate discoveries. This allows more flexibility in network discovery configurations, without manual dependency checks.

To disable a network listed in the network inventory:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Network Inventory**.
   The **Network Inventory** page is displayed.
2. From the inventory, under **Status**, turn off the toggle.
   The **Network Successfully Disabled** message is displayed.

   When a network that is mapped to a scheduled discovery instance is disabled (after it is already mapped), the status of that network, in the discovery instance inventory, is set to **Disabled**. The overall status of a discovery instance, where at least one network is disabled, is set to **Partially success**. If all networks in a discovery instance are disabled, the discovery status if set to **Failed**.

   A discovery instance that includes a disabled network cannot be triggered for execution.

Enabling Disabled Networks in the Network Inventory

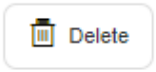
To enable a network for inclusion in the discovery instances after it has been disabled:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Network Inventory**.
   The **Network Inventory** page is displayed.
2. From the inventory, under **Status**, turn on the toggle.
   The **Network Successfully Enabled** message is displayed.

Deleting Networks Listed in the Network Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Network Inventory**.
   The **Network Inventory** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. From the network inventory list, under **Network Name**, select the checkbox(es) corresponding to the network list(s) you want to delete.
3. From the menu bar, click 

.
4. From the confirmation dialog box, click **Submit**.
   The selected network list(s) are deleted.

Discovery Configuration Settings

The **Discovery Configuration Settings** page is a centralized interface for defining how certificate and network discovery operations are conducted and reported. It is organized into the following three sections:

- Network Discovery Settings
- General Settings
- Report Settings

Details of the configuration settings in each section are covered subsequently.

Configuring Network Discovery Settings

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Settings**.
   The **Settings** page is displayed.
2. Click **+ Create**.
   The **Add** page is displayed.
3. Enter/Select the basic details.

Field descriptions for the basic details

Field	Description
***Name**	Enter a name of the setting. **Important:** This field does not support special characters.
Description	Add additional details about this scan settings.
**: Mandatory fields*	

4. Enter/Select the Network Scan Configuration details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Network Scan Configuration details

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Alive Host Detection</td><td>Select the type of host detection. The available oprions are,
• Conservative
• Balanced
• Aggresive
• Custom.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Active IP Scan</td><td>Enable this option to detect and scan active IPs.</td></tr>
<tr><td>Detection Mode</td><td>Choose the method to detect the active hosts.
• Default Ports
• ICMP only
• Custom Ports.</td></tr>
<tr><td>Scanning Speed</td><td>Adjust the scan intensity.

Note: Enabled this option if Active IP Scan = Enable

.</td></tr>
<tr><td>Concurrent Probes</td><td>Define the maximum number of simultaneous probes sent during a scan.

Note: Enabled this option if Active IP Scan = Enable</td></tr>
<tr><td>Host Timeout</td><td>Determine the wait time.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td> Note: Enabled this option if Active IP Scan = Enable</td></tr>
<tr><td>Maximum Retry</td><td>Specify the number of retry.
 Note: Enabled this option if Active IP Scan = Enable</td></tr>
</table>
</td></tr>
<tr><td>Open Port Configuration</td><td>Configure the open port.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Scanning Intentsity</td><td>Adjust the scan intensity.</td></tr>
<tr><td>Packets per Second</td><td>Set the packets.</td></tr>
<tr><td>Concurrent Parallel Probes</td><td>Determine the number of probes.</td></tr>
<tr><td>RTT Timeout</td><td>Set the RTT timeout.</td></tr>
<tr><td>Max Retries</td><td>Set the number of retry.</td></tr>
<tr><td>Probe delay</td><td>Determine the wait time.</td></tr>
<tr><td>Host Timeout</td><td>Set host timeout.</td></tr>
</table>
</td></tr>
<tr><td>OS Check Configuration</td><td>Enable the OS check radio button.
 Note: Below options will be enabled this option if OS Check Configuration = Enable</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Scanning Intentsity</td><td>Set the intensity of OS and service detection scan.</td></tr>
<tr><td>Service Detection</td><td>Determine how deeply services running on open ports are analyzed.</td></tr>
<tr><td>OS Scan</td><td>Set the OS Scan.</td></tr>
<tr><td>Version Probe Intensity Level</td><td>Set the probe intensity level.</td></tr>
<tr><td>Probe delay</td><td>Set the probe delay.</td></tr>
</table>
</td></tr>
<tr><td>Advanced Configuration</td><td>Configure the advanced configuration.
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>IPs per Batch of Discovery</td><td>Define how IPs to scan at once.</td></tr>
<tr><td>Scan Ports</td><td>Select the type of ports. The available options are,
• All Ports
• Custom Ports
• Standard Ports
• Frequently Used Ports.</td></tr>
<tr><td>TLS version(s)</td><td>Define the TLS version.</td></tr>
<tr><td>Execute Batches Sequentially</td><td>Select the checkbox to execute the batches.</td></tr>
<tr><td>Interval Between Batches</td><td>Set the interval time.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

5. Click **Save**.

Configuring General Discovery Settings

The **General Discovery Settings** section of the **Discovery Configuration :: Settings** page let you manage the general behavior of network discoveries.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To configure the general discovery configuration settings, enable/disable the following features, as required:

Field descriptions for the general discovery settings

Field	Description
Discover Private Key	To fetch private keys from endpoints as part of the discovery results, turn on the **Discover Private Key** toggle. While this feature is disabled by default to preserve confidentiality, fetching private keys from endpoints is required if you want to push the discovered certificates to new endpoints.
Synchronize Network Connectors	To ensure that the configuration and status of all associated network connectors is regularly synchronized, turn on the **Synchronize Network Connectors** toggle. If this feature is enabled, the discovery instance will attempt to sync device data with the latest connector state before scanning.
Number of Discovery History Required	Enter the number of discovery iterations to retain per job. Entries older than the specified number will be auto-purged. **Default value**: 5 **Maximum value**: 5
Access Control Scheduled Discoveries	To restrict access to scheduled discoveries to the discovery owner's user group, turn on the **Access Control Scheduled Discoveries** toggle.
**: Mandatory fields*	

Configuring Discovery Report Settings

The **Report Settings** section of the **Discovery Configuration :: Settings** page lets you define the compliance and vulnerability insights that should be included in the discovery reports.

To configure the discovery report settings, enable/disable the following features, as required:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the general discovery settings

Field	Description
Identify if MTLS is enabled on HTTPS endpoints	To check if mutual TLS (mTLS) is configured on the discovered HTTPS endpoints, turn on the **Identify if MTLS is enabled on HTTPS endpoints** toggle. This means that both, the server and the client, must provide valid certificates for authentication.
Check ciphers enabled on endpoints	To check if the supported ciphers are enabled on the discovered endpoints, turn on the **Check ciphers enabled on endpoints** toggle. In addition to discovering the ciphers, enabling this feature will also categorize them according to their security strengths in the discovery report and trigger additional scans, if required.
Check CAA records	To query the DNS for Certificate Authority Authorization (CAA) records associated with discovered domains, turn on the **Check CAA records** toggle. These records are then evaluated against the issuing Certificate Authorities to verify that certificates have been issued only by CAs explicitly authorized for those domains.
Check for Heart Bleed, Poodle and Roca Vulnerabilities	To check if there are legacy TLS vulnerabilities (such as heart bleed, POODLE, and ROCA) associated with the discovered certificates, turn on the **Check for Heart Bleed, Poodle and Roca Vulnerabilities** toggle.
**: Mandatory fields*	

Deleting Network Settings

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Settings**. The **Settings** page is displayed.
2. From the network inventory list, under **Name**, select the checkbox(es) corresponding to the network list(s) you want to delete.
3. From the menu bar, click Delete.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the confirmation dialog box, click **Submit**.
   The selected settings list(s) are deleted.

> **Note:** Default settings cannot be deleted. Additionally, any setting mapped to a network cannot be removed.

Cloning Network Settings

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Configuration** > **Settings**.
   The **Settings** page is displayed.
2. Select the checkbox that to be cloned from the settings list.
3. From the menu bar, click the **Clone** button.
   The confimation window appears.
4. Enter the new settings name that to be cloned.
5. Click **Submit**.
   The pop-up message appears as **Selected Network Settings Cloned Successfully**.

Syncing Certificates with Network Devices or Servers

It is important to ensure that the onboarded certificates are in sync with network devices. AppViewX has a cron job called **Device and Certificate synchronization** that, on being triggered, will fetch the config and update the data.

This cronjob syncs the configuration file for the eligible devices and refreshes the list of certificates available in the inventory of that device.

> **Note:** The device must be managed in AppViewX.

By default, the **Device and Certificate synchronization** cron job runs at 3AM every day. The schedule and frequency of the cron job can be customized.

- Viewing the Device and Certificate Synchronization Cron Job
- Modifying the Device and Certificate Synchronization Cron Job

Viewing the Device and Certificate Synchronization Cron Job

To view the **Device and Certificate Synchronization** cron job:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Job Scheduler**.

The **Job Scheduler** page is displayed. The **Device and Certificate synchronization** cron job is listed on this page, along with its details.

Modifying the Device and Certificate Synchronization Cron Job

To modify the **Device and Certificate Synchronization** cron job:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Job Scheduler**.
   The **Job Scheduler** page is displayed. The **Device and Certificate synchronization** cron job is listed on this page, along with its details.
2. Under **Task Name**, click **Device and Certificate synchronization**.
   The **Device and Certificate synchronization** pop-up window is displayed.
3. Enter the following details:

Field descriptions for the details

Field	Description
***Description**	Enter a description of what the cron job is for.
***Time Zone**	From the dropdown list, select the time zone in which this cron job will be scheduled.
***Occurrence Type**	From the dropdown list, select a frequency from the following options: • **Daily** • **Weekly** • **Monthly** • **Minutes**
***Starts On**	**Note:** This field is **not** displayed when **Occurrence Type** = **Minutes**. Click (**Calendar** widget) to select a date on which the cron job will be triggered.
Repeat	**Note:** This field is displayed when **Occurrence Type** = **Daily**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the number of times the cron job should be triggered in a day. When **Occurrence Type** = **Minutes**, from the **Repeat** dropdown list, select the interval between two triggers in minutes
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day(s) of the week on which you want the cron job to be triggered.
Summary	Displays a summary of the selections made for scheduling the cron job
**: Mandatory fields*	

4. Click **Update**.
   The details of the cron job are updated on the **Job Scheduler** page.

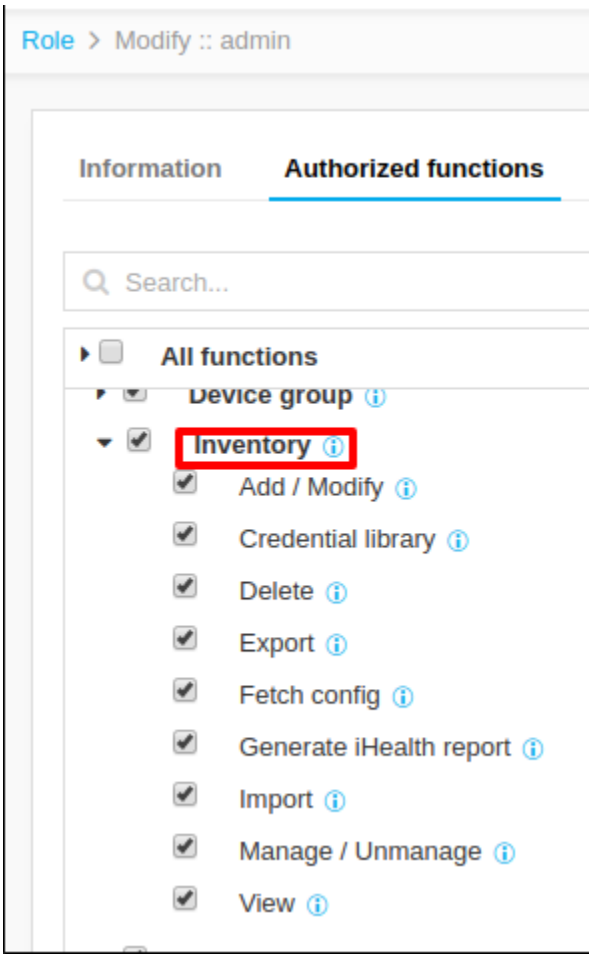
Manage Devices

- Inventory Actions
- Device Prerequisite
- ADC Prerequisite
- Firewall and Web Application Firewall (WAF) Prerequisite
- Prerequisites for Cloudflare - AppViewX CLM
- Server Prerequisite

Inventory Actions

To do any actions in the inventory, the user should have ACF permissions to access the inventory page and its various actions as mentioned in the screenshot.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- Manually Fetch the Configuration for a Device
- Delete Device
- Export Device Details
- Import Devices
- Customizing Columns
- Manage Device
- Pagination
- Unmanage Device

Manually Fetch the Configuration for a Device

If the latest configuration in the device needs to be pulled into AppViewX, those devices can be selected, and fetch config can be triggered. AppViewX will communicate with the device and pull the latest configuration available in the device and persist in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To manually get the configuration for a device,

1. Go **Menu** > **CERT+** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
2. If the device is not listed on the screen, run a search to locate it.
3. Click the checkbox beside the device name. If you want to fetch configurations for multiple devices of the same type, select their checkboxes too.
4. Click (**Fetch Con fig**) from the command bar.
5. A notification appears at the top of the screen stating, "**Fetch config has been triggered for the device.**

Delete Device

To delete the device from the inventory,

1. Go **Menu** > **CERT+** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
2. Select the desired device to delete.
3. Click the **Delete** button in the Command bar.
   The **Delete** confirmation modal appears.
4. Click **Yes** to delete the selected device.

> **Note:** To discard the deletion, click **No**. The device details and configurations will be permanently deleted from AppViewX. If the deleted device is onboarded again, it will be considered as onboarding a new device.

Export Device Details

The device details that are available in the Device Inventory page can be exported into an Excel file.

To export the details of one or more devices,

1. Go **Menu** > **CERT+** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
2. If the device you want to export is not listed on the screen, run a search to locate it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click the checkbox beside the device name. If you are exporting details of multiple devices of the same kind, select the checkboxes for each one.
4. Click the **Export** icon in the Command bar at the upper right of the screen.
5. On the **Export** pop-up screen that appears, select the type of information you want to export.
   - **All Columns** - Select this option if you want to export all information about the device.
   - **Displayed columns** - Select this option if you want to export only the information that is visible on the Device screen. This is useful if you need to compare values or settings for different devices and do not have any need to see the less important data.
   - **Columns to modify data and import** - Select this option if you are exporting device details to make modifications and then re-import the data into the Device Inventory.
6. On the screen that opens, select the location where you want the device details file to go, then click **Save**.
7. The details are then downloaded as an Excel `<.xls>` file.

Import Devices

Device import provides a hassle-free experience in onboarding multiple devices into AppViewX in one single step. For onboarding multiple devices, the details should be filled in the excel sheet in the predefined format and can be uploaded to AppViewX and from there AppViewX will dynamically onboard all the devices available in the sheet.

To import devices using a `<.csv>` file,

1. Go **Menu** > **CERT+** > **Inventory** > **Device**.
2. Click the **Import** icon in the Command bar.
3. On the Import screen that appears, navigate to the location of the import file, then select it.
4. Click **Import** to add the devices and their details to the Inventory.

Note: When the file is uploaded with improper structure or incorrect data, the import process will terminate with the errors highlighted.

Customizing Columns

The columns in the Device Inventory page are highly customizable as per the user's convenience. Any column can be hidden, added, or alter in the order of columns.

To customize columns,

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

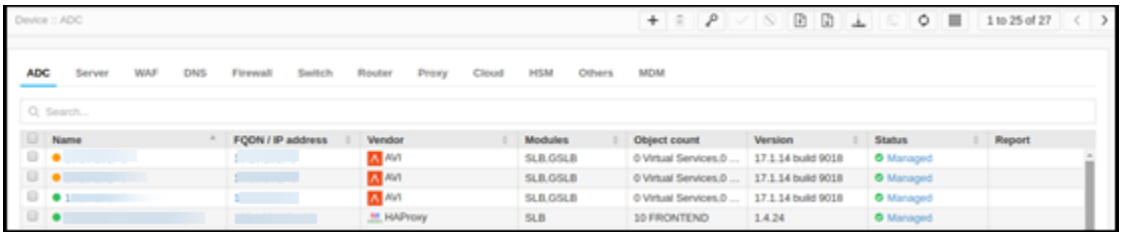
1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. Click the **Columns** icon in the Command bar.
   The **Columns** pop-up opens.
4. In the Columns pop-up, you can modify the columns by doing any of the following or in combination:
   a. Select or deselect the desired columns to be displayed.
   b. Alter the order of the column by dragging the column name to the desired order.
   c. Select all the available columns by clicking the **Select all** checkbox.
   d. Reset to the previous column selection by clicking the "**Reset to previous column selection**".
5. Click the **Save** button.

> **Note:** The saved column selection/order changes only at the user level and will remain the same until user changes it again.

6. Click the **Cancel** button to discard the changes.

Validating the Column selection

Once the user selects the columns to be displayed on the inventory page and saves the data, the device inventory page will be reloaded again with the selected columns.



Manage Device

To manage devices,

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.

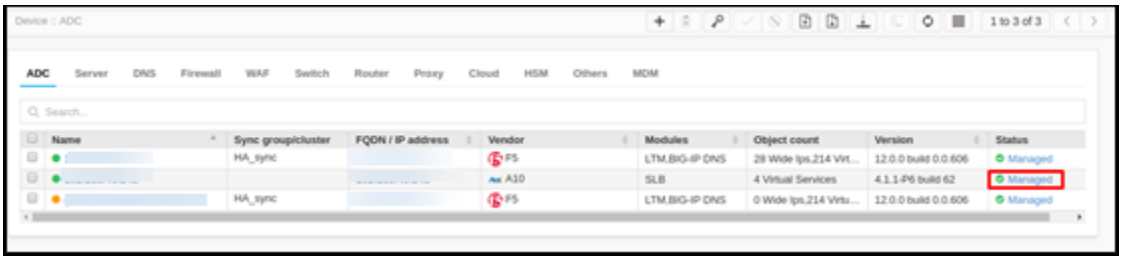
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. If the device you want to manage is not listed on the screen, run a search to locate it.

> **Note:** If you try to manage a device that is already in managed state or unmanaged a device that is already in an unmanaged state, an error message appears at the top of the screen.

Validating the Manage Action

Once the devices are moved from Unmanaged status to Managed status, the config fetch will be triggered to those devices and the device status will be updated.



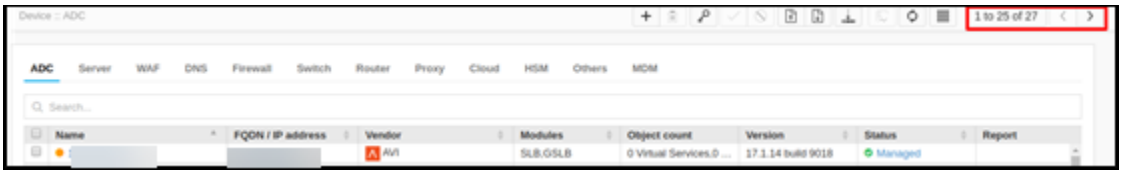
Pagination

Pagination is being used to display many devices into discrete pages. So, the user can configure the number of device details to be displayed on a page and he can navigate to the previous and the next page using the previous and the next icon.

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.

   By default, the **ADC** tab opens.

3. Select the number of records to be displayed on the device inventory page.



4. Select the Previous or Next icon to move to the previous or next page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Unmanage Device

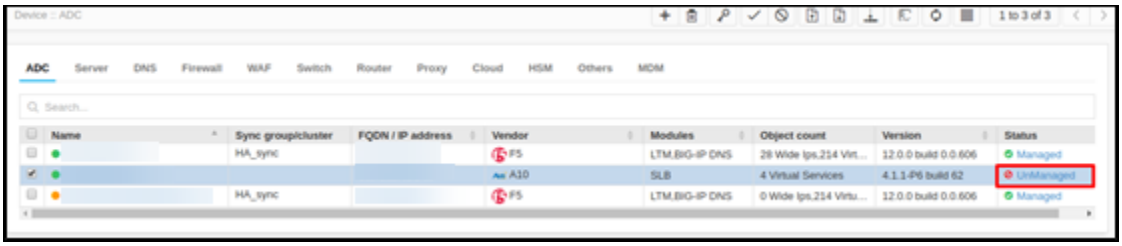
This action is being used to move the device to the unmanaged status from the managed status in the AppViewX application. If the devices are in ‘Unmanaged’ status, the midnight config fetches, and other features like Syslog, Statistics, Write actions will be disabled for those devices.

1. Log in to AppViewX application with valid credentials.
2. Click the **Menu** > **Inventory** > **Device**.
   By default, the **ADC** tab opens.
3. **Note:** If you try to manage a device that is already in managed state or unmanaged a device that is already in an unmanaged state, an error message appears at the top of the screen.

   If the device you want to unmanage is not listed on the screen, run a search to locate it.
4. Click the checkbox beside the device name.
5. To start managing the device, click the Unmanage button in the Command bar at the top of the screen.

Validating the Unmanaged Action

Once the devices are moved from Unmanaged status, the config fetch will be triggered to those devices and the device status will be updated.



Device Prerequisite

A user can discover applications or configurations and certificates associated with the applications from devices. For this CERT+ needs to login to the devices using its credentials. Devices can be inventoried on CERT+ by adding them under relevant categories of devices such as ADC, Servers, Firewall, WAF, or Cloud. Following are some prerequisites that a user has to ensure while adding the device to Inventory.

ADC Prerequisite

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	A10	AVI	Akamai	Array
IP Address/FQDN	IP Address/FQDN	IP Address/FQDN **Note:** Device must not be added with Cluster IP.	Not Applicable	IP Address/FQDN
User Privilege	• CLI/WEB/xAPI access • Read/write access	• Super-user access • System admin role for all the tenants.	• Client token • Client Secret • Access Token • Host URL	API access
Credential List	AppViewX	• AppViewX • CyberArk • Thycotic	Not applicable	AppViewX
Enable Password	Required	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Not Applicable	Not Applicable	No
Services and Port for AppViewX communication	Port number: 22, 88, and 443	Port number: 22, 443, and 5514 (to receive Syslog on AppViewX from AVI)	Port number: 443 (Outbound from AppViewX to Manage Device and Perform Akamai Actions.)	A port is required to configure access to APIs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	A10	AVI	Akamai	Array
				Note: Any port can be configured as needed.
Internet Access/Proxy if required	Not Required	Not Required	Required	Not Applicable
Location from which the certificates are discovered if Certificate Managed	No specific location	No specific location(use API's to get certificate details)	Not Applicable	Not Applicable

Supported Vendors	Amazon ELB	BigIQ	Cisco	Citrix
IP Address/FQDN	Not Applicable	IP Address	IP Address	IP Address and FQDN
User Privilege	• Access Key • Secret Key • Region	• Username/Password • Credential List • AppViewX/CyberArk	• Username/Password	• Username/Password • Credential List • AppViewX/CyberArk Role: Superuser access
Credential List	• AppViewX • Cloud account	• AppViewX • CyberArk	• AppViewX • CyberArk	• AppViewX • CyberArk

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Amazon ELB	BigIQ	Cisco	Citrix
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Yes	Not Applicable	No
Services and Port for AppViewX communication	Port number: 443 (Outbound Internet access is required to manage the ELB in AWS.)	Port number: 22 (SSH)	• Outbound Access from AppViewX for SSH service • HTTPS service	• Outbound Access from AppViewX for SSH and HTTPS service (Default/ Custom Port Information) is required • Outbound access to port 5514 is required for Citrix Device to forward the Syslog to AppViewX
Internet Access/Proxy if required	Required	Not Required	Required, if needs to be accessed with a Public IP address.	Yes, if access via a public IP address is needed
Location from which the certificates are discovered if Certificate Managed	Not Applicable (Certificates that are assigned to the listeners will be discovered by AppViewX)	CERT+ Discovery is not supported	CERT+ Discovery is not supported	Certificates are parsed only from the /flash/nsconfig/ssl/ directory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	F5	F5XC	HAProxy	NginxPlus	Infoblox LBDN
IP Address/FQDN	IP Address/FQDN	FQDN	IP Address	IP Address/FQDN	IP Address/FQDN

User Privilege	• Admin access
	• TMSH access
	  • Username / Password
	  • Credential List AppViewx/ CyberArk/ BeyondTrust
		Admin	• Username / Password
			• Credential List AppViewx/CyberArk
				Access to Nginx Installed configuration locations and access to check the syntax of Nginx. conf and restart the Nginx service to apply changes.	• Super-user access
					or
					• Access to LBDN objects that need to be managed from AppViewX

Credential List	• AppViewX • CyberArk • HashiCorp • Thycotic • BeyondTrust	AppViewX	• AppViewX • CyberArk • BeyondTrust	• AppViewX • CyberArk • HashiCorp	AppViewX
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Yes	No	Yes	Yes	Not Applicable
Services and Port for AppViewX communication	Port number: 22 and 443	Not Applicable	Port number: 22 (SSH)	Port number: 22 and any custom port for stats	Port number: 443 or custom port to access API calls

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	F5	F5XC	HAProxy	NginxPlus	Infoblox LBDN
Internet Access/ Proxy if required	Not Required	Internet access required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed	/config/filestore/ files_d/<partition>_d/ certificate_d/ /etc/ httpd/conf/ssl.crt/ /etc/ pki/tls/certs/ V10 /config/ssl/ssl.crt/ /etc/ httpd/conf/ssl.crt/ /etc/ pki/tls/certs/	NA	CERT+ Discovery is not supported	/etc/nginx/conf.d/ or any custom location	Not Applicable

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Firewall and Web Application Firewall (WAF) Prerequisite

General prerequisites

- Confirm that communication between AppViewX and the firewall is active.
- Provide an internet or proxy connection for AppViewX to interact with the firewall via REST API.
- Ensure that valid firewall account details, such as API tokens/keys and user credentials, are available.
- Grant the API admin permissions to read and modify SSL certificates.

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
IP Address/ FQDN	IP address / FQDN	IP address / FQDN	IP address /FQDN	IP address /FQDN	IP address / FQDN
User Privilege	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• User assigned an Admin Role Profile with Configuration, Operational Requests, Commit, and Import privileges for the XML API. • Username / Password • Credential List AppViewx/ Cyberark	• User assigned an Admin Role Profile with Configuration, Operational Requests, Commit, and Import privileges for the XML API. • Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark
Enable Password	Required	Not Required	Not Required	Not Required	Required
License Check	Not Required	Not Required	Not Required	Not Required	Not Required
Services and Prot for AppViewX communication	Port number: 22 (SSH)	Port number: 22 (SSH)	Port number: 443 (API)	Port number: 443 (API)	Port number: 22 (SSH, till R77) and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
					443 (API, from R80)
Internet Access/Proxy if required	Not Required	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed.	Certificates are fetched by issuing a direct command to the device through SSH.	Not supported	Certificates are fetched by issuing a direct API call to the device.	Certificates are fetched by issuing a direct API call to the device.	Certificates are fetched by issuing a direct command to the device through SSH. Directory in the device are / web/conf/ server.crt /web/conf/ server.key
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Checkpoint MDS	Fortigate	Fortimanager	Big-IP AFM	Big-IP ASM
IP Address/ FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN
User Privilege	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark
Enable Password	Required	Not Required	Not Required	Not Required	Not Required
License Check	Not Required	Not Required	Not Required	Not Required	Not Required
Services and Prot for AppViewX communication	Port number: 22 (SSH, till R77) and 443 (API, from R80)	Port number: 22 (SSH)	Port number: 443 (API)	Port number: 443 (API)	Port number: 22 (SSH) and 443 (API)
Internet Access/Proxy if required	Not Required	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed.	Certificates are fetched by issuing a direct command to the device through SSH. Directory in the device are /web/conf/ server.crt	Certificates are fetched by issuing a direct command to device through SSH.	Not supported	/config/ filestore/files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/pki/ tls/certs/ V10	/config/ filestore/files_d/ <partition>_d/ certificate_d/ /etc/ httpd/conf/ ssl.crt/ /etc/pki/ tls/certs/ V10

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Checkpoint MDS	Fortigate	Fortimanager	Big-IP AFM	Big-IP ASM
	/web/conf/ server.key			/config/ssl/ ssl.crt/ /etc/httpd/ conf/ssl.crt/ /etc/ pki/tls/certs/	/config/ssl/ ssl.crt/ /etc/httpd/ conf/ssl.crt/ /etc/ pki/tls/certs/
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Prerequisites for Cloudflare - AppViewX CLM

Cloudflare - AppViewX CLM refers to an integration between Cloudflare's services and AppViewX's Certificate Lifecycle Management (CLM) solution. This integration would combine Cloudflare's robust security and performance capabilities with AppViewX's comprehensive certificate management features.

Prerequisites

- Must have an active Cloudflare SAAS account
- Internet/ Proxy connection is required at AppViewX environment for communication between Cloudflare and AppViewX and it happens through the Rest API.
- AppViewX public ip should be whitelisted in the firewall.
- Valid Cloudflare account details like **API Tokens/API Keys.**
- Supported Certificate Format: PEM.

Roles and Permissions

- The API Tokens/ API Keys must have **Zone edit and Zone SSL Certificates-edit**access permissions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Rest API Endpoints

- The API is accessed by making HTTPS requests to a specific version endpoint URL, using GET, POST, PUT, PATCH, and DELETE methods to interact with the available information.
- Every endpoint is accessed only via the SSL-enabled HTTPS (port 443) protocol. The latest version is **Version 4**.
- The stable base URL for all Version 4 HTTPS endpoints is https://api.cloudflare.com/client/v4/.
- Requests can be authenticated using either of the following methods:
  - **API Tokens**: Include Authorization: Bearer accessToken in the request header.

```
curl -X GET "https://api.cloudflare.com/client/v4/zones/cd7d0123e3012345da9420df9514dad0" \
    -H "Content-Type:application/json" \
    -H "Authorization: Bearer YQSn-xWAQiiEh9qM58wZNnyQS7FUdoqGIUAbrh7T"
```

  - **API Keys**: Include `X-Auth-Key` and `X-Auth-Email` in the request headers.

```
curl -X GET "https://api.cloudflare.com/client/v4/zones/cd7d0123e3012345da9420df9514dad0" \
    -H "Content-Type:application/json" \
    -H "X-Auth-Key:1234567893feefc5f0q5000bfo0c38d90bbeb" \
    -H "X-Auth-Email:example@example.com"
```

Device Management

Navigate to **Inventory** > **Device** > **WAF**.

General Information for device addition:

- Account name
- Data center
- Cert Sync (Monitored/ Managed/ Ignored)

Credential Types and Authentication Methods:

- **Credential Type**: (Manual / AppViewX / CyberArk)
  - **Manual**: There are two methods of authentication for APIs.
    - **Token-Based Authentication**: Requires entering the API token.
    - **Username & Password Authentication**: Requires entering the username and password.
  - **AppViewX**: Integration with the AppViewX vault.
  - **CyberArk**: Integration with the CyberArk vault.

- Secondary device addition is not applicable.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

List of APIs Used at Backend

- **https://api.cloudflare.com/client/v4/user/tokens/verify**: Used for credential validation and device communication.
- **https://api.cloudflare.com/client/v4/zones**: Used to list account and zone details.
- Account ID, account name, zone ID, zone name, custom certificate quota, and permission details are parsed and saved in AppViewX.
- Device communication messages and other status messages are listed based on the above API responses:
  - Device communication and status messages
  - List of accounts and their details
  - List of zones and their details
  - Certificate quota and SSL permission details.

Discover Operation

- Certificate content is not discovered from Cloudflare due to API restrictions.
- Only specific certificate attributes are discovered: [Resource ID, Zone ID, Host Name, Issuer, Signature, Bundle Method, Priority, Uploaded, Modified, and Expiry time of SSL Certificate].
- The following API is used to discover certificate attributes from a particular zone using the ZoneID in the request:
  - **https://api.cloudflare.com/client/v4/zones/6812dae14999809307c0df2f23b50924/custom_certificates**
- Device profiles are created based on the zone name in the format: **[{AppViewX_AccountName}:@{CloudFlare_AccountName}:@{ZoneName}:@{ZoneId}]**

Push Operation

- Cloudflare only accepts publicly trusted certificates of the following types:
  - SHA256WithRSA
  - SHA1WithRSA
  - ECDSAWithSHA256.
- Certificates are parsed and checked for validity before being accepted. Each certificate uploaded must:
  - Be encoded in PEM format.
  - Not expire in less than 14 days from the time of upload.
  - Have a Subject Alternative Name (SAN) matching at least one hostname in the zone where it's being uploaded.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Use a private key with a minimum length (currently 2048 bits for RSA and 225 bits for ECDSA).
- Be publicly trusted by a major browser unless the User Defined bundling method is used.

Backend APIs in Use

1. POST Method API for Pushing New Certificates:
   - **API Endpoint:** https://api.cloudflare.com/client/v4/zones/023e105f4ecef8ad9ca31a8372d0c353/custom_certificates
   - This API endpoint is used to push new certificates.

```
curl -X POST https://api.cloudflare.com/client/v4/zones/023e105f4ecef8ad9ca31a8372d0c353/custom_certificates \
  -H "Authorization: Bearer 17b9lxqsnSvQrnyvYdvur8h_Fu6N0iKOirMRuECk" \
  -H "Content-Type: application/json" \
  --data '{"certificate":"-----BEGIN CERTIFICATE-----\n cert content \n-----END CERTIFICATE-----\n","private_key":"-----BEGIN RSA PRIVATE KEY-----\n
key content\n-----END RSA PRIVATE KEY-----\n" ,"bundle_method":"ubiquitous", "geo_restrictions":{"label":"us"},"type":"sni_custom"}'
```

2. PATCH Method API for Replacing Existing Certificates:
   - **API Endpoint:** https://api.cloudflare.com/client/v4/zones/6812dae14999809307c0df2f23b50924/custom_certificates/76e0e95c-2e20-44a8-b60e-fd919c9b1445
   - This API endpoint is used to replace the existing certificate identified by the certificate ID in the request.

```
{
  "certificate": "-----BEGIN CERTIFICATE-----\nMIIG...\n-----END CERTIFICATE-----",
  "private_key": "-----BEGIN PRIVATE KEY-----\nMIIJQ...\n-----END PRIVATE KEY-----",
  "bundle_method": "force",
  "geo_restrictions": {
    "label": "us"
  },
  "type": "sni_custom"
}
```

Connectors Page Field Definitions

On the Connectors page, the following fields are defined:

- **Certificate Type**: Only supports PEM format.
- **Bundle Method**: Dropdown values include Compatible, Modern, and User Defined.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **API Request Data Mapping Values for Bundle Method**:
  - Compatible maps to ubiquitous
  - Modern maps to Optimal
  - User Defined maps to force.

- **Private Key Restriction**: Dropdown values include:
  - Distribute to all Cloudflare data centers
  - Distribute only to U.S. data centers
  - Distribute only to E.U. data centers
  - Distribute only to highest security data centers.
  - API Request Data Mapping Values for Private Key Restriction:
    - No-input (Default), us, eu, highest_security.

- **Legacy Client Support**: Dropdown values are Modern and Legacy.
  - API Request Data Mapping Values for Legacy Client Support: sni_custom & legacy_custom

- **Overwrite**: Checkbox option.
  - If selected, it will replace the existing certificate.
  - If not selected, it will add a new certificate based on the quota value.

Certificate Operations

Bind Operation:

- Since this process involves importing certificates at the zone level, the Bind operation is not applicable.

Backup Operation:

- Since certificate content cannot be discovered from Cloudflare, the Backup operation is not applicable.

Rollback Operation:

- Since the Backup operation is not applicable, reverting back to an existing certificate is not possible.
- Currently, similar to other WAF devices, the rollback operation involves removing the pushed certificate. Users can then push the same certificate again through the connector if it exists in the AppViewX inventory.

Reference

For more information, visit Cloudflare API Documentation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Server Prerequisite

Supported Vendors	Apache	Apache Tomcat	Microsoft IIS	Microsoft PC	Microsoft Server	Oracle Weblogic
Operating System	All Linux Flavor	All Linux Flavor	Windows	Windows	Windows	All Linux Flavor
IP Address/ FQDN	IP Address	IP Address	FQDN or Hostname	FQDN or Hostname	FQDN or Hostname	IP Address
User Privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Local admin or Domain Admin • Allow logon locally in Windows agent machine	• Username / Password • Local admin or Domain Admin • Allow logon locally in Windows agent machine	• Username / Password • Local admin or Domain Admin • Allow logon locally in Windows agent machine	• Username / Password • Admin or sudo user privilege
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Services and Port for AppViewX Communication	Port number: 22 (SSH)	Port number: 22 (SSH) and Reset Port	Port number: 5985 (Powershell), 135 (Native API/WMI) , 445 (network drive), 8999 (Appviewx agent	Port number: 5985 (Powershell), 135 (Native API/WMI) , 445 (network drive), 8999 (Appviewx agent	Port number: 5985 (Powershell), 135 (Native API/WMI) , 445 (network drive), 8999 (Appviewx agent	Port number: 22 (SSH)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Apache	Apache Tomcat	Microsoft IIS	Microsoft PC	Microsoft Server	Oracle Weblogic
			port), and 49152-65535 (WMI/native dynamic port)	port), and 49152-65535 (WMI/native dynamic port)	port), and 49152-65535 (WMI/native dynamic port)	
Internet Access / Proxy If Required	Not Applicable	Not Applicable	Need access to Agent installed in Client env	Need access to Agent installed in Client env	Need access to Agent installed in Client env	Not Applicable
Enter Path/ Location	Customized	Customized	Not Applicable	Not Applicable	Customized	Yes, Weblogic Dir path
Location from which Certificates are discovered If Certificate managed	Certificates defined under Virtualhost of <httpd.conf> File location	Certificates defined under Connector tag of <server.xml> File location	Windows Store	Windows Store	Centralized File System	Keystore/ truststore entry defined in <config.xml> File location
Support for SNI Feature	Yes	No	Yes	Not Applicable	Not Applicable	No
Multiple Instance Support	Yes	Yes	Not Applicable	Not Applicable	Not Applicable	Yes
Supported Cert Format	<.pem>, <.crt>, and <.cer>	<.pem>, <.crt>, <.cer>, <.jks>, <.keystore>, and <.truststore>	<.pfx>	<.pfx>	<.pem>, <.crt>, <.cer>, <.jks>, <.pfx>, and <.der>	<.jks>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Oracle IPlanet	IBM Websphere	IBM Data Power	Linux	Domino
Operating System	All Linux Flavor	All Linux Flavor	All Linux/ Windows Flavor	All Linux Flavor	Windows
IP Address/FQDN	IP Address	IP Address	IP Address	IP Address	FQDN
User Privilege	• Username / Password • Admin or sudo user privilege • Wadm username and password	• Username / Password and wasadmin Username/ pasword • Admin or sudo user privilege	• GUI Username / Password/ • Rest port • Admin or sudo user privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Admin or sudo user privilege
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Services and Port for AppViewX Communication	Port number: 22 (SSH)	Port number: 22 (SSH) and Reset Port	Port number: 22 (SSH)	Port number: 22 (SSH)	Port number: 22 (SSH)
Internet Access / Proxy If Required	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Enter Path/ Location	Yes, Wadm installation Path	Yes,Websphere Dir path	Not Applicable	Yes	Yes
Location from which Certificates are discovered If Certificate managed	Keystore/ truststore entry defined in <config.xml> File location	Keystore/ truststore entry defined in <security.xml> File location	Cert/Local/ Pubcert/ SharedCert folder of IBM DATAPOWER	Customized Location	<.kyr> Location
Supported SNI feature	No	No	No	No	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	Oracle IPlanet	IBM Websphere	IBM Data Power	Linux	Domino
Multiple Instance Support	No	No	No	Not Applicable	Yes
Supported Cert Format	<.jks>	<.jks>	All format of certificates(except <jks> and <kdb>)	All format of certificates	All format of certificates

Supported Vendors	JBoss	Nginx Webserver	RabbitMq	Arbor	HPiLo
Operating System	All Linux Flavor	All Linux Flavor	All Linux Flavor	APS 6.0.0 (build IFNK) (arch x86_64)	Windows and Linux
IP Address/ FQDN	IP Address	IP Address	IP Address	API Link	IP Address
User Privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Admin or sudo user privilege	• Username / Password • Admin or sudo user privilege	HSM must be initialized and the user must have access to APS API	Username/ Password
Enable Password	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
License Check	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Services and Port for AppViewX Communication	Port number: 22 (SSH)	Port number: 22 (SSH)	Port number: 443	No	Port number: 22 (SSH)
Internet Access / Proxy If Required	Not Applicable	Not Applicable	Not Applicable	Need Access to the appliance API	Not Applicable

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Vendors	JBoss	Nginx Webserver	RabbitMq	Arbor	HPiLo
Enter Path/ Location	No	Customized	Customized	HSM must be initialized	Not Applicable
Location from which Certificates are discovered If Certificate managed	Certificates defined under Connector/ sslrealam tag of standalone <.xml> File location	Certificates defined under Server Block of <nginx.conf> File location	Certificates defined under plugins of <rabbitmq.conf> File location	Via API	Not Applicable
Supported SNI feature	No	Yes	No	No	No
Multiple Instance Support	No	Yes	No	No	No
Supported Cert Format	<.jks>	<.pem>, <.crt>, and <.cer>	<.pem>, <.crt>, and <.cer>	<.pem>	<.pem>

Certificate Actions

For launching any new application in an enterprise, an SSL certificate is required to secure the communication. The certificate lifecycle has different phases starting from enrolling. AppViewX Cert+ enables you to manage every action that is involved in the certificate lifecycle.

In the Certificate Action section, the following actions can be performed:

- Enrolling Certificates
- Renewing Certificates
- Pushing Certificates to Devices
- Reissuing Certificates
- Revoking Certificates
- Regenerating Certificates
- Reinstating Certificates
- Duplicating Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

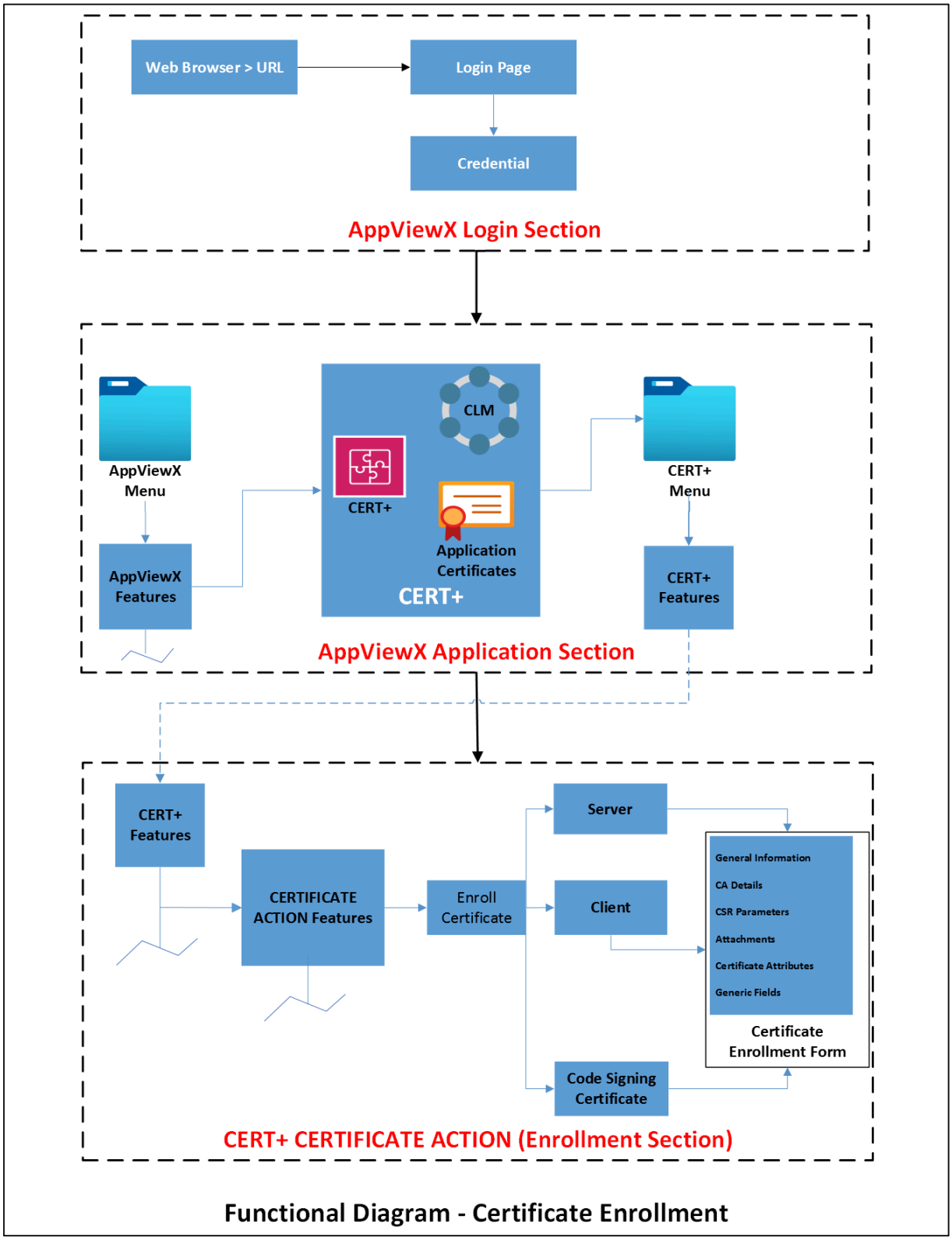
- Running Revocation Check-OCSP
- Generating Certificate Signing Request (CSR)
- Migrating CAs (CA Switch)
- Running the SSL Checker for a Certificate

Enrolling Certificates

Certificate enrollment is a process of requesting digital identity for a server or an individual from the Certificate Authority (CA). It is a primary step in certificate lifecycle management (CLM). In the enrollment process, a user must submit the details of the entity (server/individual) to the certifying authority. The authority validates the correctness of the information and ownership before issuing a digital certificate and issues a certificate.

Note: For enrolling with a CA, the respective account details must be added in AppViewX. For more details, refer to Add a CA Account section in Configuring CA Settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Functional Diagram - Certificate Enrollment

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Enrolling a Server Certificate
• Enrolling a Client Certificate
• Enrolling a Code Signing Certificate

Enrolling a Server Certificate

Important: Effective October 1st, 2025, DigiCert CA server certificates will include only server authentication in the Extended Key Usage (EKU). Dual authentication will no longer be supported.

As a temporary provision till May 01st, 2026, DigiCert CA will allow dual authentication in the EKU. Customers who need to continue enrolling server certificates with dual authentication enabled can contact the AppViewX's Site Reliability Engineering (SRE) team at saashelp@appviewx.com.

However, it is strongly recommended to transition away from the use of server certificates for dual authentication to align with industry best practices.

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Important: For CSR generation at endpoint, for **Category** = **Server** and **Vendor** = **LinuxServer**, in the endpoint application connector created after the certificate is issued, the following fields (explained here) are auto-populated/enabled and cannot be modified:

- **Category**
- **Vendor**
- **Key Location**
- **Private key in Device**

Additionally, the available profiles are filtered for the device profile selected at the time of certificate enrollment here.

Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates

For DNS providers that don't support automatic challenge verification of DNS TXT records, you are required to manually create the DNS TXT record.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: DNS providers that support automatic challenge verification can also opt for manual verification, if and as required.

To do this:

1. Activate the **Enable DNS Automation** version of the **certificate_new_request** workflow.
   To do this:

   a. Go to (**Menu**) > **Automation** > **Workflow** > **Design**.
   The **Workflow** page is displayed.

   b. To change the workflow version, turn off the toggle key to disable the **certificate_new_request** workflow.

   c. Once it is disabled, click the **certificate_new_request** workflow card to open the workflow view.

   d. In the workflow view, from the dropdown list on the menu bar, select **Version List**.
   The **Version List** dialog box is displayed.

   e. From the **Version List** dialog box, select the **Enable DNS Automation** version.
   The workflow view for the selected version is displayed.

   f. From the top right corner of the workflow view, click **ON**.

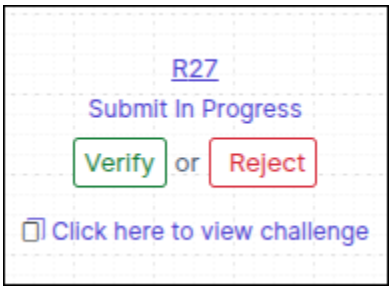
   g. In the **Confirmation** dialog box displayed, click **Validate & Enable**.
   The **Confirmation** dialog box is updated to display the message **There is an active workflow version running. Do you wish to activate & enable this version for request generation?**

   h. Click **Yes**.
   The **Enable DNS Automation** version of the **certificate_new_request** workflow is activated and the workflow is enabled.

   Note: On the **Workflow** page, validate if the **certificate_new_request** workflow is enabled. If not, turn on the toggle key to enable the workflow.

2. In the server certificate enrollment process, from the **Challenge Verify** dropdown list, select **Manual**, as explained here.
   Once the enrollment process is initiated, the **Enable DNS Automation** version of the workflow is triggered and the prompt shown in the image below is displayed on the holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



3. Click the **Click here to view challenge** prompt.
   The **Copy Token** dialog box is displayed.
4. To manually add the DNS TXT record, follow the instructions given in the **Copy Token** dialog box.
5. After creating the DNS TXT record in the corresponding DNS configuration, close the **Copy Token** dialog box.
6. On the holistic view, click **Verify**.
7. Enter your comments in the text field displayed (optional) and click **Yes**.
   The **Submit Manual TXT record update in progress** message is displayed on the holistic view.

   AppViewX validates if the DNS TXT record is updated correctly. If the validation is successful, the enrollment request is moved to the CA verification stage.

References

- Creating and managing certificate V3 extension profiles in Futurex
- Creating and managing approval groups in Futurex

What's Next

After Enrolling the certificates, you can now:

- Go to the certificate inventory to view and manage the certificates.
- Automate certificate lifecycle management by enabling:
  - Auto renewal of certificates
  - Auto regeneration of certificates
  - Auto push of certificates to endpoints
  - Alerts to notify events and status changes related to the certificates

Enrolling a Client Certificate

Client certificate enrollment refers to the process of creating a digital ID for an individual/device for authentication/encryption purposes. It follows the same process as a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: These certificates cannot be hosted on clients.

Important: In compliance with recent updates from the CA/Browser Forum S/MIME Baseline Requirements, for DigiCert-issued S/MIME certificates, it is now mandatory to include the first name and last name, or a pseudonym in the subject information during certificate enrollment.

However, in the current implementation:

- The discovery feature does not retrieve these values in the metadata.
- The upload certificate feature is not compatible with this enhancement since it does not have with a direct mapping to the certificate type, unless the certificate is discovered via a Certificate Authority scan.

To enroll a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

References

- Creating and managing certificate V3 extension profiles in Futurex
- Creating and managing approval groups in Futurex

What's Next?

To automate certificate lifecycle management for enrolled certificates:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Enable auto regeneration of certificates.
- Enable auto push of certificates to endpoints. To do this, add an application connector to push the certificate to an AWS device and select the **Push Automatically** checkbox.
- Set alerts to be notified of all events and statuses of the certificates.

Enrolling a Code Signing Certificate

Code Signing certificate enrollment refers to the process of creating a digital ID for a code or document. It starts with the generation of a key pair (private and public key) and CSR and then submitting the CSR to the desired CA to procure a certificate. CERT+ supports the generation of key pair on the device, HSM, and AppViewX. You can also upload the CSR for enrolling for a digital certificate.

Note: These certificates cannot be hosted on servers.

To enroll a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Code Signing Certificate**.
   The **Enroll Code Signing Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Options	Description
***Certificate Authority**	Select the desired certificate authority from the dropdown lists. Based on the selected CA, other CA details are configured. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
	If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	This field will be shown only for Digicert CA. Select the division to which the certificate must be enrolled.
Certificate Profile	This field is applicable only for AppViewX CA and Google CA. Select the Profile to which the Certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	This is applicable only for Google CA. Select the location of the issuer CA from the dropdown.
***Issuer Name**	This is applicable only for Google CA. Select the name of the issuer CA from the dropdown.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
	From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given. To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
	• **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: While enrolling certificates with policies using Google CA, the following points must be considered.

Certificate Enrollment - Strict Policy

- The Common Name will not be pre-filled from the policy.
- The following validation will be seen based on strict policy guidelines.
  - If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.

Certificate Enrollment - Suggestive Policy

- The Common Name will not be pre-filled from the policy
- The following validation will be seen based on strict policy guidelines.
  - If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
  - If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.

4. For the EJBCA CA, enter/select the **Vendor Specific Details**.

Field descriptions for the Vendor Specific Details section.

Field	Description
End entity user name	Enter the name of the end entity.
*** End Entity Profile Name**	Select the profile name from the dropdown list.
*** User Common Name**	Select the common name from the dropdown list.
*** Certificate Profile Name**	Select the certificate profile name from the dropdown list.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR parameters

Field	Description
Common Name	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-). **Note:** The common name field is made optional. You can now enroll and perform CLM actions for code signing certificates without a common name.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters for their operational purposes.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.

    Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

Once the certificate is issued successfully, the certificate will be retrieved into AppViewX.

References

- Creating and managing certificate V3 extension profiles in Futurex
- Creating and managing approval groups in Futurex

What's Next?

To automate certificate lifecycle management for enrolled certificates:

- Enable auto regeneration of certificates.
- Enable auto push of certificates to endpoints. To do this, add an application connector to push the certificate to an AWS device and select the **Push Automatically** checkbox.
- Set alerts to be notified of all events and statuses of the certificates.

Renewing Certificates

Digital certificates are issued with a limited validity period. Before the expiration of their validity, the certificates have to be renewed and placed on the server for service continuity. The renewal process is specific to CAs, depending on their operations. The result is be the issuance of the certificate with extended validity. CERT+ enables you to trigger certificate renewal in different ways. You can trigger renewal from the certificate inventory or the certificate details and its provisioned details can be verified and trigger the renewal from a holistic view. Group policy auto-renewal takes care of the certificate renewal automatically and it can be combined with auto-push for hassle-free automation.

You can renew the certificates via the Certificate Inventory section also.

Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

Note: GoDaddy SSL certificates can be managed only via the SSL credits in your GoDaddy account. To renew GoDaddy certificates, refer the instructions given here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Renewing a Server Certificate
- Bulk Renewing Server/Client Certificates
- Renewing a Client Certificate
- Tracking Certificate Renewal via the Process Explorer
- Enabling Auto Renewal for Discovered Certificates

Renewing a Server Certificate

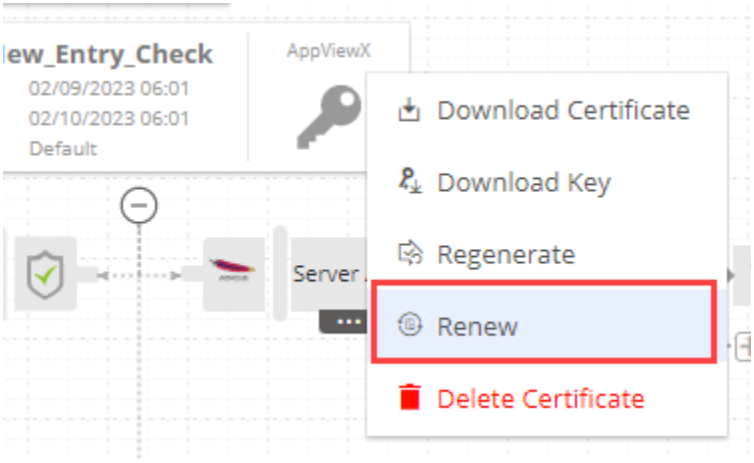
Note: From v2021.1.0, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

Important: To renew Microsoft Azure Enterprise Application self-signed certificates, follow the instructions given here.

If you are renewing a single certificate, you can trigger the renewal from the holistic view as they can verify all the details before initiating the renewal.

To renew a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. To open the holistic view of a certificate, under **Common Name**, select the required certificate name.
3. From the **(More)** menu for the certificate, click **Renew**.



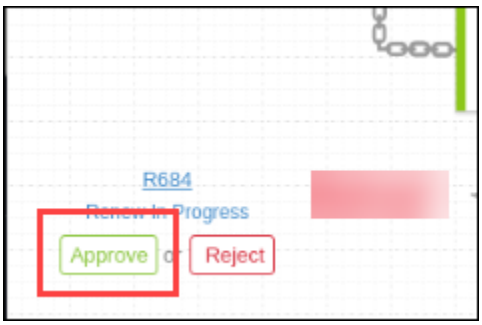
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Server Certificate** > **Renew** page is displayed. The fields on this page are displayed depending on the type of certificate and the issuing certificate authority.

4. On the **Server Certificate > Renew** page, update the renewal details if and as required.
   For field descriptions, you can refer to the instructions for enrolling a server certificate.

> **Note:** Starting version 2023.1.0 FP2, for certificates issued by Entrust and Microsoft, you can upload a new CSR in the **CSR Generation** field.
> • If you are uploading a new CSR, ensure that the new and existing **Common Name** in the **CSR Parameters** are the same.

5. Click **Renew**.
   The **Renew** dialog box is displayed.
6. Enter your comments in the text field and click **Yes**.
   A request ID, which is the work order ID, is generated automatically, and work order status is displayed adjacent to the certificate in the holistic view. If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
7. Click **Approve** to proceed.



   The **Approve** dialog box is displayed.
8. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

9. Click **Yes**.
   Once the approval process is complete, the **Implement** option is displayed in the holistic view.
10. Click **Implement**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Implement** dialog box is displayed.

11. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
12. Click **Yes**.
    The renewal process is triggered. After renewal is completed, the workflow status updates to **Completed**.

Bulk Renewing Server/Client Certificates

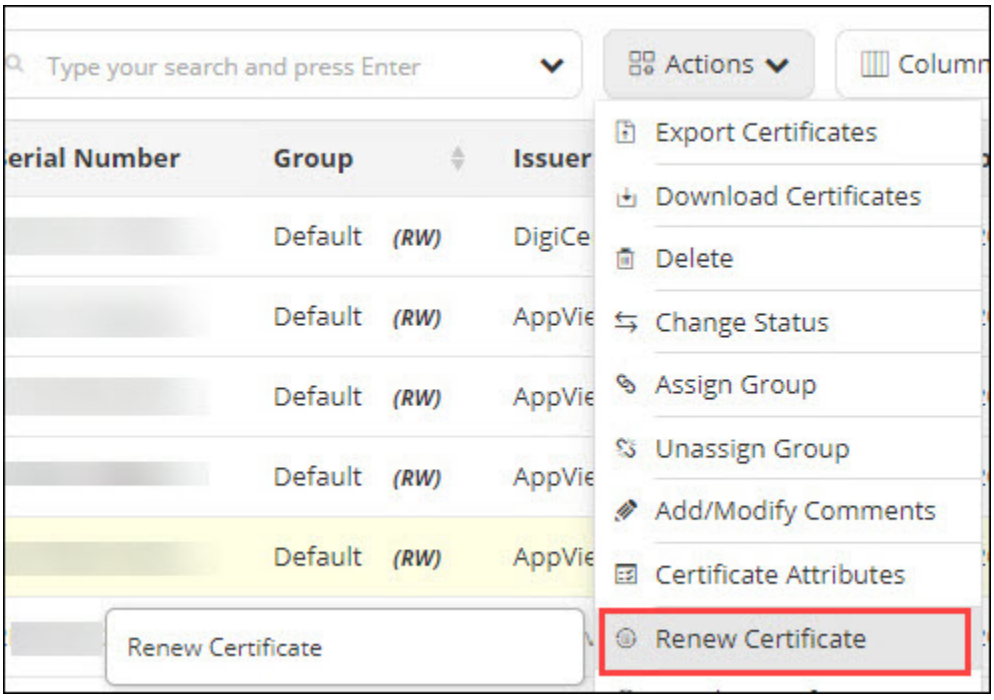
Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

Bulk renewal of the certificates can be triggered from the inventory by selecting more than one certificate.

To renew server certificates in bulk:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Server** / **Client**.
   The **Server/Client Certificate** page is displayed.
2. Under **Common Name**, select the checkboxes corresponding to all the certificates you want to renew.
3. From the **Actions** dropdown menu, click **Renew Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



The **Renew Certificate** dialog box is displayed.

4. From the following options, select when do you want to **Renew Selected Certificate(s)**:

   a. To immediately renew the selected certificate(s), select **Now**.

   • Certificate renewal request, for the selected certificate(s), will be triggered immediately.

> **Note:**
> • Certificates with the work order status in progress or with read-only permission will be skipped.
> • In case of Digicert certificates, the certificates will be auto-reissued unless the Order validity is expired.

OR

   b. To schedule an automatic renewal for a later time, select **Set auto-renew**.

   c. In the **Renew Certificates** _____ **Days before Expiry** field, to specify how many days before their expiry the selected certificate(s) should be renewed, enter a value between **1** and **120**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Assuming that you have entered **120** in this text field, certificates with validity less than 120 days will be triggered for renewal within the next **6 hours**.

> **Note:**
> - Certificates with the work order status in progress or with read-only permission will be skipped.
> - In case of Digicert certificates, the certificates will be auto-reissued unless the Order validity is expired.

5. Click **Submit**.
   Depending on the selections made in the **Renew Certificate** dialog box, the certificate renewal process will be triggered.

> **Note:** The status of the renewal process is monitored using the **Process explorer**.

Renewing a Client Certificate

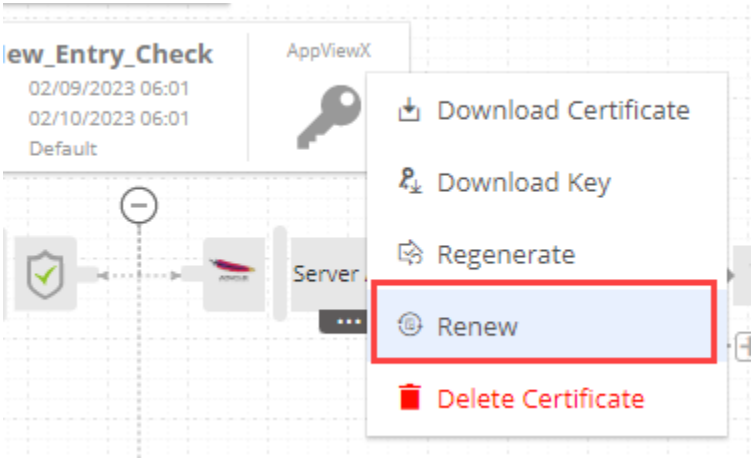
Note: v2021.1.0 onwards, AppViewX provisions the renewal functionality for certificates issued via Google CA. This is done by utilizing the certificate's existing CSR or private key details.

If you are renewing a single certificate, you can trigger the renewal from the holistic view as they can verify all the details before initiating the renewal.

To renew a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Client**.
   The **Client Certificate** page is displayed.
2. To open the holistic view of a certificate, under **Common Name**, select the required certificate name.
3. From the **(More)** icon for the certificate, click **Renew**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

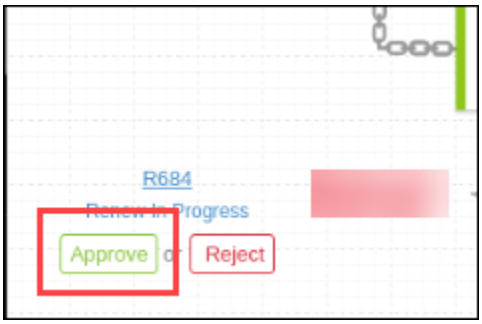


The **Client Certificate** > **Renew** page is displayed. The fields on this page are displayed depending on the type of certificate and the issuing certificate authority.

4. On the **Client Certificate > Renew** page, update the renewal details if and as required.

> **Note:** Starting version 2023.1.0 FP2, for certificates issued by Entrust and Microsoft, you can upload a new CSR in the **CSR Generation** field.
> - If you are uploading a new CSR, ensure that the new and existing **Common Name** in the **CSR Parameters** are the same.

5. Click **Renew**.
   The **Renew** dialog box is displayed.
6. Enter your comments in the text field and click **Yes**.
   A request ID, which is the work order ID, is generated automatically, and work order status is displayed adjacent to the certificate in the holistic view. If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
7. Click **Approve** to proceed.



The **Approve** dialog box is displayed.

8. Enter your comments in the text field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

9. Click **Yes**.
   Once the approval process is complete, the **Implement** option is displayed in the holistic view.
10. Click **Implement**.

   The **Implement** dialog box is displayed.
11. Enter your comments in the text field.
   If the workflow request has to be implemented automatically in the future, click **Schedule later** .
12. Click **Yes**.
   The renewal process is triggered. After renewal is completed, the workflow status updates to **Completed**.

Tracking Certificate Renewal via the Process Explorer

The **Process Explorer** is a listing of all certificates scheduled for renewal on present day and certificates awaiting approval for renewal. Once a certificate is renewed, it is removed from this listing. The **Process Explorer** is useful for monitoring the renewal status especially in the case of bulk renewals.

To access the process explorer:

Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Renew Certificate** > **Process Explorer**.
The **Renew Certificate** page with the listings is displayed.

Enabling Auto Renewal for Discovered Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Renewal

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

What's Next?

For automating the certificate lifecycle management, in addition to auto renewal, you can:

- Enable auto regeneration of certificates.
- Enable auto push of certificates to endpoints. To do this, add an application connector to push the certificate to an AWS device and select the **Push Automatically** checkbox.
- Set alerts to be notified of all events and statuses of the certificates.

Pushing Certificates to Devices

Pushing certificates refers to the automated distribution and deployment of digital certificates. You can enable certificates to be pushed at the time of adding an application connector.

> **Note:** Users can push certificates to Akamai CPS only when the CSR is generated on the end point.

- Adding Application Connectors
- Pre - and Post - Push Script Usage Steps
- Pushing a Server Certificate to a Device
- Pushing a Client Certificate to a Device
- Pushing an Intermediate Certificate to a Device
- Pushing a Root Certificate to a Device
- Enabling Auto Push of Certificates to Endpoints
- Bulk Push for Intermediate/Root Certificates

Adding Application Connectors

An application connector is a software application running on a server. To add the application connector, the application should be managed under the AppViewX device inventory. All the supported devices in the AppViewX inventory can be provisioned with the certificate by adding the connector. The connector enables certificate provisioning for cloud-managed devices.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Users can push certificates to Akamai CPS only when the CSR is generated on the end point.

- Adding Application Connectors for Servers
- Adding Application Connectors for Cloud Connectors
- Adding Application Connectors for Cloud Devices
- Adding Application Connectors for Firewalls
- Adding Application Connectors for MDMs
- Adding Application Connectors for ADC Devices

Adding Application Connectors for Servers

AppViewX supports creating an application connector for the following server vendors:

- ABAP
- ADFS Server
- Akamai CPS
- Arbor
- Apache (Linux)
- Apache (Windows)
- Cisco CallManager
- CiscoIOS
- CiscoISE
- CiscoUCS
- IBM Client (Linux)
- IBM Client (Windows)
- IBM Data Power
- IBM Domino
- IIS
- ILO
- iPlanet
- Java
- JBoss

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Linux Server
- Microsoft PC
- Microsoft Server
- MQServer
- MQClient (Windows)
- MQServer (Windows)
- MS SQL
- MySQL
- Nginx
- Rabbit MQServer
- VMWare
- Web Dispatcher
- Weblogic (Linux)
- Weblogic (Windows)
- Websphere (Linux)
- Websphere (Windows)
- Tomcat (Linux)
- Tomcat (Windows)
- PingFederate

ABAP

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **ABAP**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ABAP server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Service Restart	To restart the ABAP service immediately after the certificate is pushed, enable this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For ABAP, this field is enabled by default and is non-editable.

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

ADFS Server

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **ADFS Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ADFS Server devices already onboarded in AppViewX.

3. Enter the **Certificate Details**.

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the ADFS server, or a URL from where the ADFS server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Name**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. For JKS certificates, a keystore is a repository used for storing private keys and certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the **KeyStore Name** field, enter the name of the JKS keystore in which the certificate to be pushed is stored.
***KeyStore Password**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
User	Enter the details of the user that has the necessary permissions to push the certificate.
Group	Enter the details of the user group that has the necessary permissions to push the certificate.
Password Version	Enter the version of the algorithm that is used to encrypt the password for accessing the ADFS server.
Alias Name	This field is displayed when **Certificate Type** has one of the following values: • PKCS#12 (*.pfx) • PKCS#12 (***.p12)*** • PKCS#12 (_Cert) • CERTDB (*.db) Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate File Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the intermediate certificate file.
***CA File Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the root certificate file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information populated here, the **Server selection** section is populated with the list of available ADFS Server devices already onboarded in AppViewX.

4. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Push Details**.

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. The script that automates the push operation is called a push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script Parameters	Enter the values that will be passed to the pre-push script.
***Push Script File Name**	Enter the name of the push script.
Push Script Parameters	Enter the values that will be passed to the push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post Push Script Parameters	Enter the values that will be passed to the post-push script.
Post Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Rollback Location	To recover from a conflict or failure during a push operation, copies of the certificate and configuration file are stored in a directory or storage location. In the **Rollback Location** field, enter the path to this location.
Rollback Parameters	Enter the rollback parameters (settings) used to initiate the rollback process.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Akamai CPS

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Akamai CPS**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Akamai CPS server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed. For Akamai CPS, by default, the **PEM (*.pem)** certificate is selected and the dropdown list is non-editable.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox. For Akamai CPS, this feature is enabled by default and the field is non-editable.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For Akamai CPS, this feature is enabled by default and the field is non-editable.

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Arbor

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Arbor**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Arbor server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate File Name**	Enter the file name of the certificate (with the extension) to be pushed.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Apache (Linux)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Apache**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Apache (Linux) server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Service Restart	To restart the Apache service immediately after the certificate is pushed, enable this checkbox.
Suppress Heartbeat Alerts During Service Restart	Enabling this option to disable or prevent false alert triggered during Apache service. **Note:** • This field is disabled when Service Restart selected. • To view or update default setting, go to: **Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings**.
Heartbeat File Path	Specify the hearbeat file path. **Note:** This field is enabled when Suppress Heartbeat Alerts During Service Restart is checked.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
Intermediate Location	This field is displayed when **Push Root and Intermediate Certificates** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the path to the location on your local system where the intermediate certificate file is stored.
Root Location	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the path to the location on your local system where the root certificate file is stored.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Apache (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows Apache**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows Apache devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Intermediate Location	Enter the path to the location on your local system where the intermediate certificate file is stored.
Root Location	Enter the path to the location on your local system where the root certificate file is stored.
Service Restart	To restart the Apache service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.

   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Cisco CallManager

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Cisco CallManager**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Cisco Call Manager devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Restart Service(s)	To restart the Cisco CallManage service(s) immediately after the certificate is pushed, enable this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

CiscoIOS

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **CiscoIOS**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Profile Selection** section is populated with the list of available Cisco IOS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Profile Selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Trustpoint Name**	For Cisco IOS devices, a trustpoint configuration is an element that includes details related to a certificate such as the certificate file, the private key file, the CA certificate, and other settings related to the certificate. In the **Trustpoint Name** field, enter the name of the trustpoint configured on the Cisco IOS device(s) to which the certificate will be pushed.
Push Root Certificates	To push the root certificate, along with the end certificate, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For Cisco IOS devices, the intermediate certificates are automatically included in the certificate chain.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

CiscoISE

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **CiscoISE**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Cisco ISE devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing server configuration XML file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
Friendly Name	Enter the certificate friendly name assigned in the CSR generated for requesting/enrolling the certificate
Used By	From the dropdown list, select the purpose for which the certificate will be used.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root certificate, along with the end certificate, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

CiscoUCS

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **CiscoUCS**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Cisco UCS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Key ring**	A key ring configuration stores the keys and certificates used for encryption and authentication. Enter the name of the key ring configuration on the Cisco UCS server.
Trust point	A trustpoint configuration is used to manage certificates on a Cisco UCS server. In the **Trust point** field, enter the name of the trustpoint configured on the Cisco UCS server(s) to which the certificate will be pushed.

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

IBM Client (Linux)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **IBMClient**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available IBM Client (Linux) devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the IBM Client server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

IBM Client (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows IBMClient**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows IBM Client devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the Windows IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Windows IBM Client server, this feature is enabled by default and the field is non-editable.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

IBM Data Power

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **IBMDataPower**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available IBM data Power devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Push Location	From the dropdown list, select the file type of the certificate to be pushed.
Certificate Location	Enter the path to the location on your local system where the certificate file to be pushed is stored.
Key Location	The private key associated with a certificate is stored in a key file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Intermediate Location	Enter the path to the location on your local system where the intermediate certificate file (for the end certificate being pushed) is stored.
Root Location	Enter the path to the location on your local system where the root certificate file (for the end certificate being pushed) is stored.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

IBM Domino

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **IBMDomino**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available IBM Domino devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Push Location	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server from where the server can retrieve the certificate.
KYR Password	Enter the password to the key ring file (KYR file), which stores the keys and certificates used for encryption and authentication.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

IIS

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **IIS**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Push Certificate Type**	Select from the following options: • **Push Certificate** You can only push certificates to the Certificate store or Centralized File System. • **Push and Bind Certificate** You can push a certificate to the Certificate store and bind it to the IIS site.

Based on the information entered here, the **Server selection** section is populated with the list of available IIS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select where the certificate to be pushed is located: • **Certificate Store**: A repository that stores certificates and their associated keys • **Centralized file system**: A file server that stores certificate files
Certificate Store	This option is displayed only when **Location Type** = **Certificate Store**. Within the certificate store, select the location where the certificates are stored from the following options: • **Personal store**: A location where user-specific certificates, such as those used for encryption and authentication, are stored • **Web hosting store**: A location where certificates used for web server configurations are stored
***Friendly name**	Enter the certificate friendly name assigned in the CSR generated for requesting/ enrolling the certificate
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Bind type**	**Note:** This field is displayed when the **Push Certificate Type** is selected as **Push and Bind Certificate**. To manage the SSL/TLS certificates for websites, select a bind type from the following options: • **Update Certificate Only**: Update the SSL/TLS certificate used by an existing site binding on the web server. It replaces the current certificate with a new one without modifying any other settings associated with the site binding (such as the hostname or port). • Update Site Binding: Update the SSL/TLS settings for an existing site binding on the web server. It allows you to update not only the certificate but also other settings associated with the site binding, such as the hostname, port, and SSL/TLS protocol settings. • **Create New Site Binding**: Create a new site binding on the web server for the specified hostname, port, and IP address (if applicable) and associates it with the specified SSL/TLS certificate. This is typically used when you want to add a new website or domain to the web server and configure SSL/TLS settings for it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- **Certificate Store Push**
  - If the certificate is created **at the endpoint** (private key on the device):
    - The **server certificate** is pushed in **.pem** format.
    - The **root and intermediate certificates** are pushed in **.pfx** format.
  - If the certificate is created **in AppViewX** (private key within AppViewX):
    - The **server**, **root**, and **intermediate certificates** are all pushed in **.pfx** format.
- **File System Push**
  - Only a **single .pfx file** (containing the certificate, private key, and root/intermediate certificates if available) is pushed to the specified file system location.
- **Supported Certificate type for File System Push**
  - PKCS#12 (.pfx)
- When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:
  - **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
  - **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings
- File system push is supported only when the Centralized File System option is enabled on the onboarding page.
  - The Certificate Location field is optional. By default, the certificate will be pushed to the directory specified during onboarding.
  - The password for the certificate pushed to the file system is retrieved from the vault configured during onboarding.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system. **Note:** Overwrite option is disabled by default for Microsoft IIS.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

ILO

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **ILO**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ILO devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.

   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

iPlanet

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **iPlanet**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available iPlanet devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .

The **Selected devices** list is updated automatically.

4. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***Database Path**	This field is displayed only when **Customize Push Location** is selected. Enter the path to the location on your local system where the certificate and key database files are stored.
Configuration Restart	To restart the server after pushing the certificate, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Java

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Java**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information entered here, the **Server selection** section is populated with the list of available Java devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Name**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. For JKS certificates, a keystore is a repository used for storing private keys and certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the **KeyStore Name** field, enter the name of the JKS keystore in which the certificate to be pushed is stored.
***KeyStore Password**	This field is displayed when **Certificate Type** = any of the JKS certificate formats. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
User	Enter the details of the user that has the necessary permissions to push the certificate.
Group	Enter the details of the user group that has the necessary permissions to push the certificate.
Password Version	Enter the version of the algorithm that is used to encrypt the password for accessing the ADFS server.
Alias Name	This field is displayed when **Certificate Type** has one of the following values: • **PKCS#12 (*.pfx)** • **PKCS#12 (*.p12)** • **PKCS#12 (_Cert)** • **CERTDB (*.db)** Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate File Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the intermediate certificate file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CA File Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the name of the root certificate file.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. The script that automates the push operation is called a push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script Parameters	Enter the values that will be passed to the pre-push script.
***Push Script File Name**	Enter the name of the push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Script Parameters	Enter the values that will be passed to the push script.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post Push Script Parameters	Enter the values that will be passed to the post-push script.
Post Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Rollback Location	To recover from a conflict or failure during a push operation, copies of the certificate and configuration file are stored in a directory or storage location. In the **Rollback Location** field, enter the path to this location.
Rollback Parameters	Enter the rollback parameters (settings) used to initiate the rollback process.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

JBoss

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **JBoss**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available JBoss devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing **server.xml** file is used to create the application connector. (By default, this option is selected.) If it is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled). **Note:** After discovery, on editing the application connector, the use existing checkbox will be the selected/enabled state
Certificate Type	This field is displayed when **Use Existing Configuration** is enabled. From the dropdown list, select the file type of the certificate to be pushed.
***KeyStore Location**	This field is displayed when **Use Existing Configuration** is enabled and **Certificate Type** = **JKS (*.jks)**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed when **Use Existing Configuration** is disabled and **Certificate Type** = **JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Alias Name**	This field is displayed when **Use Existing Configuration** is disabled and **Certificate Type** = **Default JKS (*.jks)** or **JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Linux Server

Important: If the certificate is generated with CSR generation at endpoint, if an application connector is created for the certificate, the following fields will be auto-populated/selected and cannot be modified:

- **Category**
- **Vendor**
- **Key Location**
- **Private key in Device**

Additionally, the available profiles will be filtered for the device profile selected at the time of certificate enrollment here.

1. On the client (or) server certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **LinuxServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

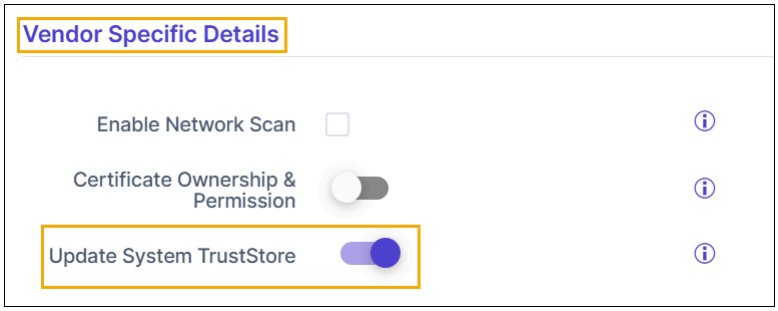
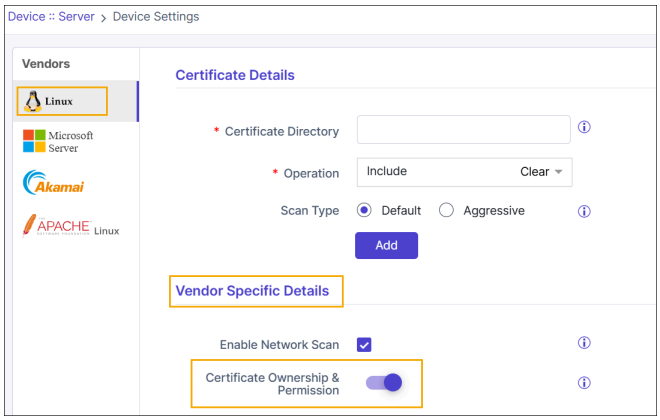
Based on the information entered here, the **SSL templates** section is populated with the list of available Linux Server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Enable Truststore Update	This field is displayed for all **PEM** certificate types. Click the radio button to enable the Update System TrustStore option for root and intermediate certificates. **Note:** By default, this option is disabled. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** > **Vendor Specific Details** section > **Update System TrustStore**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	
Certificate Ownership & Permission	Enable the toggle button to customize the certificate ownership and define the file permissions for the certificates. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** > **Vendor Specific Details** section > **Certificate Ownership & Permission**.  Field descriptions for the Certificate Ownership & Permission Details
Custom Push	This field is displayed for all **PEM** and **DER** certificate types. From the following options, select the method of pushing certificates: • **Chain**: The full certificate chain, which includes the end, intermediate, and root certificates, will be pushed to the server. • **Issuer & Server**: The server's certificate and its issuer's certificates will be pushed to the server. • **Server Only**: Only the server's certificate will be pushed to the server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Linux Server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Certificate Location	This field is displayed for all PEM, DER and PKCS#7 certificates. Enter the path to the location on your local system where the certificate file to be pushed is stored.
Key Location	This field is displayed for all PEM, DER and PKCS#7 certificates. The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***KeyStore Location**	This field is displayed for the PKCS#12 and JKS certificates. A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the keystore file, for the certificate to be pushed, is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore Password**	This field is displayed for the PKCS#12 and JKS certificates. Enter the password required to access the keystore file for the certificate to be pushed.
***Alias Name**	This field is displayed for the PKCS#12 and JKS certificates. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Truststore Location	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the certificates to be pushed, is stored. **Note:** Truststore Location can be specified without the file extension as well.
Truststore password	This field is displayed for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

Field descriptions for the Certificate Ownership & Permission Details

Field	Description
Owner	Enter the username for certificate ownership on the target device.
Owner Permission	Select the owner permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
User Group	Enter name of the user group that requires access to the certificate.
User Group Permission	Select the group permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Other User Permission	Select the other user permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Microsoft PC

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **Microsoft PC**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Certificate Store Location** section is populated with the list of available Microsoft PC devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Certificate Store Location**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate File Name**	Enter the file name of the certificate to be pushed.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.

Note:

When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Microsoft Server

Prerequisistes: When adding connectors using the Exchange Server, note the following points:

- During Microsoft Server device addition ensure that the username is added with the domain in the format—<username>@<domain>.
- The **iisreset.exe** file is expected at the default location. (C:\Windows\System32) to support IIS Service restart.
- For the certificate being enrolled, **Country name** must be provided in order to renew the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Microsoft Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ABAP server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, from the dropdown list, select one of the following options:
   - **MS Server**
   - **Exchange Server**
   - **Windows Gateway**

Note: If you have selected **Exchange Server**, profiles will be displayed in the format, **Server type : Service name : Node details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

For MS Server: Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select the location to which the certificate will be pushed: • **File System** (a storage location on your computer) • **Certificate Store** (a specialized location within the operating system for managing digital certificates)
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Credential Type**	This field is displayed for the JKS certificates. From the dropdown list, select the source of the access credentials.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	This field is displayed for the **PEM**, **DER**, and **PKCS#7** certificates. The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***KeyStore Password**	This field is displayed for JKS certificate types.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the password required to access the keystore that contains the JKS certificate to be pushed.
Alias Name	This field is displayed for the PKCS#12 and CERTDB certificate types. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private key entry password	This field is displayed for the JKS certificates. Enter the password required to decrypt the private key associated with the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate Certificate Alias Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. This field is not displayed for the JKS certificate types. Enter the alias name of the intermediate certificate file.
***Root Certificate Alias Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the alias name of the root certificate file.

For Exchange Server: Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	The certificate type is defaulted to the following values • For AppViewX CSR generation - certificates which have private key, **PKCS#12(*.p12)** is the supported certificate format. • For Endpoint CSR generation **PKCS#7(*.p7b)** is the supported certificate format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The password field in not set for **PKCS#12(*.p12)** since its a transactional password and handled by AppViewX.
***Friendly Name**	• For **PKCS#12(*.p12)** it is the user specified input. • For **PKCS#7(*.p7b)** certificate type, the friendly name is the common name of the certificate specified at the time of Endpoint CSR generation. During the push operation the common name is populated in the friendly name field (it is not editable).
Services	From the dropdown list, select one from the following services: • **POP** • **IIS** • **SMTP** • **IMAP**
Restart Service	This field is displayed only when **Services** = **IIS**. To restart the IIS service after the certificate is pushed, to ensure all changes have taken effect as required, select this checkbox.

For Windows Gateway: Field descriptions for the Certificate Details

Field	Description
Location Type	The **Certificate Store** option is selected by default—a specialized location within the operating system for managing digital certificates. (**File system** is disabled).
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. **Note:** Root and intermediate names cannot be entered for this CSR/Certificate. If auto-push is enabled for CSR, try again after the certificate is generated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings This is applicable for all service/devices such as Microsoft Server, Microsoft Exchange Server, Windows Gateway.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

MQServer

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **MQServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows Apache devices already onboarded in AppViewX.

3. Under **SSL templates**:

   a. Based on the functionality required, select the **Profile**.

   b. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	This field is displayed only for the **Create KDB** profile. Enter the name of the KDB certificate file that will be pushed to the server.
***KDB password**	This field is displayed only for the **Create KDB** profile. Enter the password required to access the KDB certificate file.
QManager Name	This field is displayed only for the **Create KDB** profile. From the dropdown list, select the name of the MQServer's queue manager.
Server Certificate Label	This field is displayed only for the **Create KDB** and **Override** profiles. This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the MQServer, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	This field is displayed for the **Create Label** profile.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Private key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

MQClient (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows MQClient**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows MQClient devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the Windows IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Windows IBM Client server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Private key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

MQServer (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows MQServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows MQServer devices already onboarded in AppViewX.

3. Under **SSL templates**:

   a. Based on the functionality required, select the **Profile**.

   b. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***KDB File Name**	This field is displayed only for the **Create KDB** profile. Enter the name of the KDB certificate file that will be pushed to the server.
***KDB password**	This field is displayed only for the **Create KDB** profile. Enter the password required to access the KDB certificate file.
QManager Name	This field is displayed only for the **Create KDB** profile. From the dropdown list, select the name of the MQServer's queue manager.
Server Certificate Label	This field is displayed only for the **Create KDB** and **Override** profiles. This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the MQServer, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Private key in device	This field is displayed for the **Create Label** profile.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Private key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

MS SQL

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **MSSQL**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available MS SQL devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed. AppViewX supports only PEM (*.crt) type as the certificate is imported to certificate store irrespective of the certificate type.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on the **MS SQL machine**, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the file path to the **private key** location on the **MS SQL machine**.
Service Restart	Enabling this option will restart the SQL Server service to apply the configuration changes. **Note:** • By default, this setting is enabled based on the global device configuration. To modify, go to: **CERT+** > **Device Management** > **Server** > **Device Settings** > **Vendors** > **Microsoft SQL**. • This feature requires Windows Gateway version v2024.1.0.0 or later. In earlier versions, the service restarts automatically by default.
Force Encryption	Enabling this option enforces encryption for all SQL server connections. **Note:** • By default, this setting is enabled based on the global device configuration. To modify, go to: **CERT+** > **Device Management** > **Server** > **Device Settings** > **Vendors** > **Microsoft SQL**. • This feature requires Windows Gateway version v2024.1.0.0 or later. In earlier versions, the service restarts automatically by default.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: **Bind Operation in AppViewX for MS SQL:** During the **bind operation**, AppViewX updates the registry with the following keys: • **Certificate Thumbprint Key**: Stores the thumbprint of the pushed certificate. • **ForceEncryption Key**: Set to **1** to enable encryption for the SQL instance. After updating these keys, the **SQL service is restarted** to apply the changes.

Note:
When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.

   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

MySQL

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **MySQL**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information entered here, the **SSL templates** section is populated with the list of available MySQL devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Intermediate Location**	Enter the path to the location on your local system where the intermediate certificate file (for the end certificate being pushed) is stored.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Nginx

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Nginx**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Nginx devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Rabbit MQServer

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **RabbitMQServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information entered here, the **SSL templates** section is populated with the list of available Rabbit MQServer devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Intermediate Location**	Enter the path to the location on your local system where the intermediate certificate file (for the end certificate being pushed) is stored.
Private key passphrase	Enter the password required to access the private key file.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

VMWare

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **VMWare**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available VMware devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Selected devices** list is updated automatically.

4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Web Dispatcher

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **WebDispatcher**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Web Dispatcher devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
PSE Type	From the dropdown list, select the file type of the certificate to be pushed.
Service Restart	To restart the Web Dispatcher service immediately after the certificate is pushed, enable this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For the Web Dispatcher server, this field is enabled by default and is non-editable.

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Weblogic (Linux)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Weblogic**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Weblogic devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Truststore Location**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored. **Note:** The AppConnector cannot be saved if the KeyStore and TrustStore locations are the same.
***Truststore Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Configuration Restart	To restart the server after pushing the certificate, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Key Location	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Weblogic (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows Weblogic**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Weblogic devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
***Key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Truststore Location**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Websphere (Linux)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Websphere**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information entered here, the **Server selection** section is populated with the list of available Websphere devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	This field is displayed only when **Customize Push Location** is selected. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	This field is displayed only when **Customize Push Location** is selected. Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Truststore Location**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. For JKS certificates, the root and intermediate certificates are stored in a truststore file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed only when **Customize Push Location** is selected and for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Key Location	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Websphere (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows Websphere**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Websphere devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Customize Push Location	To push the selected certificates to a new directory or existing location that is associated with http-listeners, select this checkbox.
***Certificate Type**	This field is displayed only when **Customize Push Location** is selected. From the dropdown list, select the certificate file type.
***KeyStore Location**	A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	Enter the password required to access the keystore file for the certificate to be pushed.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Push Root and Intermediate Certificates	This field is displayed only for JKS certificates. To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Truststore Location**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Truststore Password**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Configuration Restart	To restart the server after pushing the certificate, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Key Location	This field is displayed when the **Private Key in Device** option is selected. Enter the path to the location of the private key on the hardware device.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Tomcat (Linux)

Prerequisites

- **SFTP** is used for the push operations. Ensure that the SFTP port is open to upload or push the certificate to the target machine.

Adding an Application Connector for Tomcat (Linux)

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Tomcat**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Tomcat devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing **server.xml** file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
***Certificate Type**	This field is displayed when **Use Existing Configuration** is not selected. From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **PEM (*.crt)/PEM (*.cer)/PEM (*.pem)**. This field is displayed when the **Use Existing Configuration** is disabled.
***Key Location**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **PEM (*.crt)/PEM (*.cer)/PEM (*.pem)**. The private key associated with a certificate is stored in a key file. In this field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore Location**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **JKS (*.jks)/Default JKS (*.jks)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **JKS (*.jks)/Default JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **JKS (*.jks)/Default JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Service Restart	To restart the Tomcat service immediately after the certificate is pushed, enable this checkbox.
Push Root and Intermediate Certificates	This field is displayed when **Use Existing Configuration** is not selected. To push the root and intermediate certificates, along with the end certificate, select this checkbox.
***Root Location**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **Pem (*.crt)/Pem (*.cer)/Pem (*.pem)**. Enter the path to the location on your local system where the root certificate file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Intermediate Location**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **Pem (*.crt)/Pem (*.cer)/Pem (*.pem)**. Enter the path to the location on your local system where the intermediate certificate file is stored.
***Truststore Location**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **JKS (*jks)**. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **JKS (*jks)**. Enter the password required to access the truststore file for the JKS certificate to be pushed.
***Truststore File Name**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **Default JKS (*jks)**. Enter the name of the truststore file for the JKS certificate to be pushed.

5. Enter/select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.

   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Tomcat (Windows)

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows Tomcat**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Tomcat devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, in the **Server selection** section, from the dropdown list in **Available Devices**, select one of the following:
   - **Tomcat**: This selection displays device profiles for Tomcat. The server.xml files are updated based on the profile and the inputs selected/entered in the rest of the fields.

     The profile names use the following naming convention: **WIN_DEVICE :: Tomcat: 8443 : localhost:localhost**
   - **Default**: This selection displays the push-only profiles. The bind operation is not supported.

     The profile names use the following naming convention: **WIN_DEVICE :: Default:**
   - **ADManager**: This selection displays device profiles for ADManager. The server.xml files are updated based on the profile and the inputs selected/entered in the rest of the fields.

     The profile names use the following naming convention: **WIN_DEVICE :: ADManager: 8443 : localhost:localhost**
   - **ADSelfService**: This selection displays device profiles for ADSelfService. The server.xml files are updated based on the profile and the inputs selected/entered in the rest of the fields.

     The profile names use the following naming convention: **WIN_DEVICE :: ADSelfService: 8443 : localhost:localhost**

   Profiles are displayed based on the selection made. The **Selected devices** list is updated automatically.
4. From the profiles displayed, to select the required profiles, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled, the existing **server.xml** file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate directory**	Enter the path to the location on your local system where the certificate file (to be pushed to the server) is stored.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key directory**	The private key associated with a certificate is stored in a key file. In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Key File Name**	Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Location**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)/PKCS#12 (*.p12)/PKCS#12 (*.pfx)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***KeyStore File Name**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)**. Enter the file name of the keystore file that contains the private keys and the associated certificates. The extension **.key** is automatically populated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Password**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)/PKCS#12 (*.p12)/PKCS#12 (*.pfx)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	This field is displayed when **Certificate Type** = **Default JKS (*.jks)/PKCS#12 (*.p12)/PKCS#12 (*.pfx)**. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Service Restart	To restart the Windows Tomcat service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***CA File Name**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the root certificate.
Intermediate File or Bundle Name	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the intermediate certificate.
***Truststore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Truststore Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.
***Truststore File Name**	This field is displayed when **Certificate Type** = **Default KS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the name of the truststore file for the JKS certificate to be pushed.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

PingFederate

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **PingFederate**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name <PingFederate connector> for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.
*: *Mandatory fields*	

Based on the information entered here, the **Server selection** section is populated with the list of available PingFederate devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, in the **Server selection** section, from the dropdown list in **Available Devices**, select one of the following:
   - **SSL Authentication Certificate Profile**: TThis profile requires a certificate that must be associated from the Client Inventory. If a certificate enrolled under the Server, Code Signing, or Client category in AVX is associated, it will be pushed to the device's Client Inventory. Hence, the appropriate certificate should be bound from the Client Inventory.

     The profile names use the following naming convention: **{DeviceName:SPConnectionName:SSL Authentication Certificate}**.
   - **SSL Verification Certificate Profile**: This profile allows association with any certificate permitted by the device, but only one certificate stays active while others remain non-active. It maintains a separate inventory from Client, Server, and Code Signing. Non-active certificates use a default connector that supports push only operations. Only the certificate, not the key, can be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Active Certificate**: Only one certificate can be active.

  The profile names use the following naming convention: **{DeviceName:SPConnectionName:SSL Verification Certificate:Active}**

- **Non-active certificates**: All remaining certificates.

  Profile Name: {DeviceName:SPConnectionName:SSL Verification Certificate}

- **Digital Signature Settings Profile**: This profile requires a certificate that must be associated from the Signing Inventory of the PingFederate device. When a server, client, or code signing certificate is pushed, it is placed in the device's Signing Inventory. Since the device accepts all certificates regardless of their EKU, the binding process can proceed as long as the certificate resides in the Signing Inventory. Certificates can be associated with either the Primary or the optional Secondary signing certificate profiles.

  - **Primary Signing Certificate Profile**: The profile names use the following naming convention: **{ DeviceName:SPConnectionName:Digital Signature Settings:Primary }**

  - **Secondary Signing Certificate Profile**: The profile names use the following naming convention: **{ DeviceName:SPConnectionName:Digital Signature Settings:Secondary }**

- In addition to associating certificates with specific profiles, they are also pushed to the corresponding inventories based on their certificate category.

  The profile names use the following naming convention: **{ DeviceName }**

- **SSL Verification Certificate Profile**: This profile allows association of any certificate, as permitted by the device. Only one certificate can be active as Primary and one as Secondary at a time; others are classified as Active or Non-Active. Active certificates can be promoted to Primary or Secondary. The profile uses a separate inventory, distinct from Client, Server, and Code Signing inventories. Certificates (excluding Primary and Secondary) are supported by a default connector for push-only operations. Only certificates, not keys, can be pushed to this profile.

  - **Primary Active Certificate**: Only one certificate can be primarily active.

    Profile Naming : { DeviceName:SPConnectionName:Signature Verification Certificate:Primary }

  - **Secondary Active Certificate**: Only one certificate can be secondarily active.

    Profile Naming: { DeviceName:SPConnectionName:Signature Verification Certificate:Secondary }

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Active / Non-active certificates**: All remaining certificates.

  Profile Naming: { DeviceName:SPConnectionName:Signature Verification Certificate:Active }

- **Non-Active - Profile Naming: { DeviceName:SPConnectionName:Signature Verification Certificate }**

Profiles are displayed based on the selection made. The **Selected devices** list is updated automatically.

4. From the profiles displayed, to select the required profiles, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Private key in device	Select the checkbox if required.
*: *Mandatory fields*	

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device.
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

• To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Adding Application Connectors for Cloud Connectors

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Internal**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Cloud Connector**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **SSL profiles** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

2. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.

4. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Adding Application Connectors for Cloud Devices

AppViewX supports creating an application connector for the following Cloud device vendors:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- AWS
- Azure
- GCP

AWS

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **AWS**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
Service Types	From the dropdown list select, one of the following: • ACM • IAM • Cloudfront • ELB
***Connector Name**	Enter a name for this connector, to be able to identify it later.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Tip: AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	This field is displayed when **Vendor** = **AWS** and **Service Types** = **Cloudfront**. For CloudFront, certificates can be stored in either AWS Certificate Manager (ACM) or AWS Identity and Access Management (IAM). From the options given, select the certificate location.
Certificate ARN	This field is displayed when **Certificate Location** = **ACM**. The ARN (Amazon Resource Name) is a unique identifier assigned to each certificate that is managed by ACM. It is used to reference the certificate in API calls, policies, and so on. In this field, enter the ARN of the certificate to be pushed.
***Certificate File Name**	This field is displayed when **Certificate Location** = **IAM**. In this field, enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For AWS, this field is enabled by default and is non-editable.
Default Certificate	In the event that a certificate cannot be pushed, a default certificate is pushed as a fall back option. To enable this, select the **Default Certificate** checkbox.

5. Enter the **Certificate Tags**.
   A certificate tag is a label that you can assign to a certificate. To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

   To enter the certificate tags:

   a. **Enter Key** and **Enter Value**, in the respective fields, for the tag.

   b. Click **Add**.
      The tag, as a key-value pair, is listed in the table shown below the fields.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Azure

For Azure Services except Virtual Machines

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Azure**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
Service Types	From the dropdown list select, one of the following: • Key vault • Application gateway • App service • Enterprise Application • Api Management • App Registration • Front Door

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Target Profile	A target profile is a configuration that defines the details for integrating and pushing certificates to the target system.
	For application gateway From the dropdown list, from the following options, select a target profile for pushing a certificate to the application gateway: • **Gateway SSL Profile** (Configure TLS/SSL encryption for secure communication between gateway and clients.) • **Gateway Listener Profile** (Accept incoming HTTP/HTTPS requests on specific ports and paths.) • **Gateway Backend Settings Profile** (Route requests to specific application servers based on routing rules.)
	For app service From the dropdown list, from the following options, select a target profile for pushing a certificate to the app service: • **Bring Your Own Certificate (.pfx)** (Upload your own **.pfx** certificate, along with its private key.) • **Public Key Certificates** (Upload only the public certificate without the private key, for scenarios where the certificate will be used only for verification purposes.)
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.
**: Mandatory fields*	

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

3. To select the device(s)/profile(s) and domain(s), for Azure Front Door, to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click . The **Selected devices** list is updated automatically.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed. For **Service Types** = **Enterprise Application**, by default, the **PKCS#12 (*.pfx)** certificate type is selected and the field is disabled for editing.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Keyvault Object Type	This field is displayed when **Service Types** = **Key vault**. From the following options, select the key vault object to which the certificate will be pushed: • **Certificates** (The Azure key vault can store x509 certificates for securing communications and establishing the identity of services.) • **Secrets** (The Azure key vault secret is a secure object used for storing sensitive information, such as passwords and cryptographic keys.)
Certificate Status Enabled	This field is displayed only when **Keyvault Object Type** = **Secrets**. To enable the certificate after it is pushed to the target system, select **Yes**.
Set activation date	This field is displayed only when **Keyvault Object Type** = **Secrets**. To set an activation date for the certificate being pushed: a. Select the **Set activation date** checkbox. b. Use the calendar widget and time zone dropdown list to set the date and time for the certificate activation.
Set expiration date	This field is displayed only when **Keyvault Object Type** = **Secrets**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To set an expiration date for the certificate being pushed: a. Select the **Set expiration date** checkbox. b. Use the calendar widget and time zone dropdown list to set the date and time for the certificate expiry.
Make Certificate Active	This field is displayed when **Service Types** = **Enterprise Application**. To make the certificate being pushed the active certificate for the Enterprise Application service, select this checkbox. An active certificate is the default certificate used for securing communication, authentication, and encryption. The rest of the certificates associated with this service are categorized as inactive certificates.
Notification Email Addresses	This field is displayed when **Service Types** = **Enterprise Application**. To enter email addresses that will be notified when this certificate is pushed and/or made active: a. Click . b. Enter the required email address and press **Enter**. c. To add multiple email addresses, repeat steps **a** and **b**. Alternatively, you can use the search field to add an already entered email address.
Certificate Push Type	Certificate push type specifies the mechanism that will be used for pushing certificates to the targeted service.
	For application gateway Select one from the following options: • **Upload a Certificate to Gateway** (for uploading a new certificate) • **Replace/Update existing Certificate in Gateway** (for renewing/ replacing an existing certificate)
	For app service

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	For Azure app service, certificate push type has the following values: • **Upload a Certificate to App Service** (for uploading a new certificate) • **Replace/Update existing Certificate in App Service** (for renewing/replacing an existing certificate) **Important:** However, for Azure app service, this field is disabled for editing and the **Upload a Certificate to App Service** is selected by default.
	For Api Management For the Azure Api management service, certificate push type has the following values: • **Upload a Certificate to Api Management** (for uploading a new certificate) • **Replace/Update existing Certificate in Api Management** (for renewing/replacing an existing certificate) **Important:** However, for the Azure Api management service, this field is disabled for editing and the **Upload a Certificate to App Service** is selected by default.
Certificate Location	**For the Azure Application Gateway** From the following options, select where the certificate will be stored after it is pushed: • **Upload directly to Application Gateway**: Upload certificates directly to the Application Gateway • **Choose from Azure Key Vault**: Store certificates in Azure Key Vault and then reference them in the Application Gateway configuration.
	For Azure App Service

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select where the certificate will be stored after it is pushed: • **Upload directly to App Service** • **Choose from Azure Key Vault**: Store certificates in Azure Key Vault and then reference them in the App Service configuration.
	For Azure Api Management From the following options, select where the certificate will be stored after it is pushed: • **Upload directly to Api Management**: Upload certificates directly to the Application Gateway • **Choose from Azure Key Vault**: Store certificates in Azure Key Vault and then reference them in the Api Management configuration.
***Secret Name**	This field is displayed when **Service Type** = **Front Door**. Enter the name of the secret in Azure Key Vault that stores the certificate to be pushed to Azure Front Door.
***Key Vault Subscription ID**	This field is displayed when **Service Type** = **Front Door**. Enter (a new)/Select (from an existing list) the Azure subscription ID for the Key Vault from which the certificate is to be retrieved.
***Key Vault Name**	This field is displayed when **Service Type** = **Front Door**. From the dropdown list, select the name of the Key Vault in which the certificate is stored.
Replace Certificate in Key Vault	This field is displayed when **Service Type** = **Front Door**. Use the toggle key to specify whether an existing certificate in the specified Key Vault should be overwritten with the new one during the push operation.
***Key Vault Certificate Name**	This field is displayed when **Service Type** = **Front Door**. Enter the logical name under which the certificate is stored in the Key Vault.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For Azure Virtual Machines

For Linux-based Virtual Machines

Important: If the certificate is generated with CSR generation at endpoint, if an application connector is created for the certificate, the following fields will be auto-populated/selected and cannot be modified:

- **Category**
- **Vendor**
- **Key Location**
- **Private key in Device**

Additionally, the available profiles will be filtered for the device profile selected at the time of certificate enrollment here.

1. On the client (or) server certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **LinuxServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

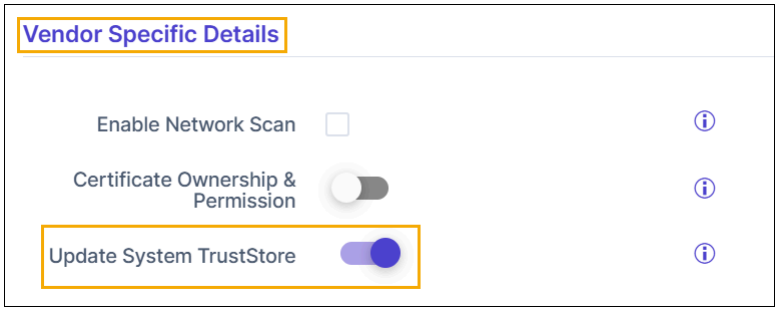
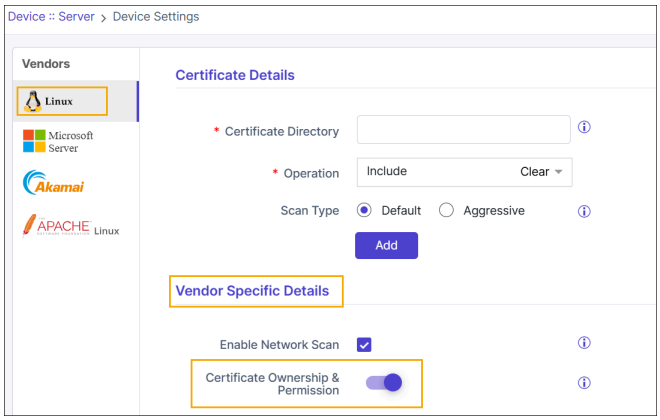
Based on the information entered here, the **SSL templates** section is populated with the list of available Linux Server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Enable Truststore Update	This field is displayed for all **PEM** certificate types. Click the radio button to enable the Update System TrustStore option for root and intermediate certificates. **Note:** By default, this option is disabled. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** > **Vendor Specific Details** section > **Update System TrustStore**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	
Certificate Ownership & Permission	Enable the toggle button to customize the certificate ownership and define the file permissions for the certificates. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** > **Vendor Specific Details** section > **Certificate Ownership & Permission**.  Field descriptions for the Certificate Ownership & Permission Details
Custom Push	This field is displayed for all **PEM** and **DER** certificate types. From the following options, select the method of pushing certificates: • **Chain**: The full certificate chain, which includes the end, intermediate, and root certificates, will be pushed to the server. • **Issuer & Server**: The server's certificate and its issuer's certificates will be pushed to the server. • **Server Only**: Only the server's certificate will be pushed to the server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Linux Server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Certificate Location	This field is displayed for all PEM, DER and PKCS#7 certificates. Enter the path to the location on your local system where the certificate file to be pushed is stored.
Key Location	This field is displayed for all PEM, DER and PKCS#7 certificates. The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***KeyStore Location**	This field is displayed for the PKCS#12 and JKS certificates. A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the keystore file, for the certificate to be pushed, is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore Password**	This field is displayed for the PKCS#12 and JKS certificates. Enter the password required to access the keystore file for the certificate to be pushed.
***Alias Name**	This field is displayed for the PKCS#12 and JKS certificates. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Truststore Location	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the certificates to be pushed, is stored. **Note:** Truststore Location can be specified without the file extension as well.
Truststore password	This field is displayed for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

Field descriptions for the Certificate Ownership & Permission Details

Field	Description
Owner	Enter the username for certificate ownership on the target device.
Owner Permission	Select the owner permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
User Group	Enter name of the user group that requires access to the certificate.
User Group Permission	Select the group permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Other User Permission	Select the other user permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

For Windows-based Virtual Machines

Prerequisistes: When adding connectors using the Exchange Server, note the following points:

- During Microsoft Server device addition ensure that the username is added with the domain in the format—<username>@<domain>.
- The **iisreset.exe** file is expected at the default location. (C:\Windows\System32) to support IIS Service restart.
- For the certificate being enrolled, **Country name** must be provided in order to renew the certificate.

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Microsoft Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ABAP server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, from the dropdown list, select one of the following options:
   - **MS Server**
   - **Exchange Server**
   - **Windows Gateway**

   Note: If you have selected **Exchange Server**, profiles will be displayed in the format, **Server type : Service name : Node details**.

4. Under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For MS Server: Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select the location to which the certificate will be pushed: • **File System** (a storage location on your computer) • **Certificate Store** (a specialized location within the operating system for managing digital certificates)
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Credential Type**	This field is displayed for the JKS certificates. From the dropdown list, select the source of the access credentials.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	This field is displayed for the **PEM**, **DER**, and **PKCS#7** certificates. The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***KeyStore Password**	This field is displayed for JKS certificate types. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
Alias Name	This field is displayed for the PKCS#12 and CERTDB certificate types.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private key entry password	This field is displayed for the JKS certificates. Enter the password required to decrypt the private key associated with the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate Certificate Alias Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. This field is not displayed for the JKS certificate types. Enter the alias name of the intermediate certificate file.
***Root Certificate Alias Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the alias name of the root certificate file.

For Exchange Server: Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	The certificate type is defaulted to the following values • For AppViewX CSR generation - certificates which have private key, **PKCS#12(*.p12)** is the supported certificate format. • For Endpoint CSR generation **PKCS#7(*.p7b)** is the supported certificate format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The password field in not set for **PKCS#12(*.p12)** since its a transactional password and handled by AppViewX.
***Friendly Name**	• For **PKCS#12(*.p12)** it is the user specified input. • For **PKCS#7(*.p7b)** certificate type, the friendly name is the common name of the certificate specified at the time of Endpoint CSR generation. During the push operation the common name is populated in the friendly name field (it is not editable).
Services	From the dropdown list, select one from the following services: • **POP** • **IIS** • **SMTP** • **IMAP**
Restart Service	This field is displayed only when **Services** = **IIS**. To restart the IIS service after the certificate is pushed, to ensure all changes have taken effect as required, select this checkbox.

For Windows Gateway: Field descriptions for the Certificate Details

Field	Description
Location Type	The **Certificate Store** option is selected by default—a specialized location within the operating system for managing digital certificates. (**File system** is disabled).
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. **Note:** Root and intermediate names cannot be entered for this CSR/Certificate. If auto-push is enabled for CSR, try again after the certificate is generated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings This is applicable for all service/devices such as Microsoft Server, Microsoft Exchange Server, Windows Gateway.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

GCP

1. On the certificate holistic view, click **Add Connector**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **GCP**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
Service Types	From the dropdown list select, one of the following: • Classic Certificates • Certificate Manager • Load Balancer
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
Upload Certificate as	• **New**: If you are uploading a new certificate to the GCP Certificate Manager, select this option. • **Update**: If you are updating a certificate existing in the GCP Certificate Manager, select this option.
Certificate Location	For **Service Types = Load Balancer**, this field is set to **Classic Certificates** and is disabled for editing. This field comes with the following options: • **Classic Certificates**: Upload your certificate and private key directly to the load balancer's configuration. • **Certificate Manager**: Reference certificates managed by Certificate Manager in your load balancer configuration.
Certificate Name	Enter the name of the certificate being pushed.
Scope of Certificate	From the following option, select the scope of the certificate being pushed: • **Global** (Certificate is available for use across all regions within a GCP project) • **Regional** (Certificate is limited to a specific region within a GCP project)
Certificate Description	Enter additional details related to the certificate being pushed.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From GCP, the script files can be stored only in AppViewX.
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Adding Application Connectors for Firewalls

AppViewX supports creating an application connector for the following Firewall device vendors:

- CheckPoint
- Cisco
- Fortinet
- PaloAlto

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Firewall**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select the required firewall vendor. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **Profile Selection** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

2. To select the device(s) to which the certificate will be pushed, under **Profile Selection**:

   a. For **CheckPoint** Vendor, to filter the available profiles, from the dropdown menu for Available profiles, select a value from the following options:
   - **Admin Portal**
   - **HTTPS Inspection**.

   b. For **PaloAlto** vendor, to filter the available profiles, from the dropdown menu for Available profiles, select a value from the following options:
   - **PaloAlto Firewall**
     - Shared location
     - SSL/TLS Service profile
     - IKE Gateways
     - SSL Inbound Inspection Profiles
     - Authentication Profiles.
   - **Panorama**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Shared location
- SSL/TLS Service profile
- IKE Gateways
- SSL Inbound Inspection Profiles
- Authentication Profiles.

c. From the list of **Available Devices** displayed, to select the target device(s) for pushing the certificate, click .

The **Selected devices** list is updated automatically.

3. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Trust Point Name**	A trustpoint configuration is an element that includes details related to a certificate such as the certificate file, the private key file, the CA certificate, and other settings related to the certificate. In the **Trustpoint Name** field, enter the name of the trustpoint configured on the target system to which the certificate will be pushed.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Password	Enter the password required to access the certificate file/trust store.
Private Key Passphrase	Enter the password required to access the private key file associated with the certificate.
Push to Firewall	To push the certificate when it is updated directly to the firewall, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Trust Type	**Important:** Trust type is applicable only for server certificates issued by private CAs with a customized template that issues certificate to the PaloAlto device with **Key Usage** as **Certificate Signing** for certificates that have a private key. **Trust Type** defines how a firewall handles SSL/TLS traffic based on whether a certificate is trusted or untrusted. Select a trust type status from the following values: • **Forward Trust** Select this option to establish the firewall as a trusted third party (proxy) to the session between the client and the server. For **Trust Type** = **Forward Trust**, if the server's certificate is valid (trusted) and signed by a known, trusted CA (like VeriSign, DigiCert, etc.), the firewall decrypts the traffic, inspects it, and then re-encrypts it using its own certificate, which is trusted by the client due to the configured CA. • **Forward Untrust** Select this option for the firewall to notify to clients when the server certificate is signed by a CA that the firewall does not trust. For **Trust Type** = **Forward Untrust**, if the server's certificate is self-signed or from an unknown CA, the firewall may re-encrypt the traffic using an untrusted certificate, causing the client to see a warning that the connection is not secure. **Note:** If the certificate trust type was already specified when configuring the certificate on the device, then upon discovery in AppViewX, the trust type field will reflect the same value as configured in the device port.

4. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a firewall certificate to the device:

- To push a firewall certificate to a device, see Pushing a Server Certificate to a Device.

Adding Application Connectors for MDMs

AppViewX supports creating an application connector for the following MDM vendors:

- MobileIron

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **MDM**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select the required vendor. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

   Based on the information populated here, the **Device Groups** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.
2. To select the device(s) to which the certificate will be pushed, under **Device Groups**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Configuration name**	Enter the name of the configuration profile that includes the certificate to be pushed. A configuration profile defines the policies for managed devices.
***Certificate Category**	Enter the name of the certificate group to which the certificate to be pushed belongs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***PFX Password**	This field is displayed for the PKCS#12 certificates. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

4. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Adding Application Connectors for ADC Devices

AppViewX supports creating an application connector for the following ADC device vendors:

- A10
- Array
- AVI
- Citrix
- F5
- HAProxy
- NginxPlus
- Radware

1. Enter the **General Information** for the ADC devices.

Field descriptions for the Certificate Details

Field	Description
***Category**	From the dropdown list, select **ADC**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select the ADC device vendor (for the device to which this certificate will be pushed). If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Based on the information populated here, the **SSL Templates/Server selection/Virtual server selection/SSL profiles** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

Note: The name of this section is populated based on the **Vendor** selected.

2. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Activate Certificate	To activate the certificate after it has been pushed, select this checkbox.
Service Action	From the dropdown list, select the required value: • **Restart** (stops and starts the process) • **Reload** (informs the daemon to reload only the configurations) • **None** **Note:** After device addition, if there are managed HAProxy certificates in the certificate inventory, by default, **Service Action** is set to **None**.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Certificate key pair name**	Enter the key-pair name used to identify the certificate and its associated private key.
Enable SNI Push for Certificate	To enable SNI push in the virtual server, select this checkbox.
Enable SNI in Virtual Server	To enable SNI in the virtual server, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For the Web Dispatcher server, this field is enabled by default and is non-editable.
Service Restart	To restart the device service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

4. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pre - and Post - Push Script Usage Steps

Prerequisites

- If the scripts are written using Python:
  - Scripts for the on-prem deployment should start with

```
#!/appviewx/dependencies/appviewx_addons/Python/bin/python
```

  - Scripts for the SaaS deployment should start with

```
#!/usr/bin/python
```

- The script input can be consumed using the command line argument `sys.argv[1]`
- The script output should be in the JSON format, generated only using the `print` statement.
-

Script Output	Script Execution Status
`AppResponseCode:0`	Success
`AppResponseCode:-1` or any other script errors	Failure

- The script should be code-signed. Please contact AppViewX Support (help@appviewx.com) to get the script code signed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Using Scripted Integrations for On-prem

1. Get the code-signed script from the AppViewX support team (help@appviewx.com). This will be a **.zip** file that includes the script and the signature.
2. Save the code-signed **.zip** file in all the AppViewX vendors pods running node file system.

   Default path: **<home>/appviewx/appviewx_dependencies/aps/**
3. Mention in the **.zip** filename in all the relevant fields in the CERT+ user interface.

> **Note:** The folder path for the file is not required. Custom folder paths are restricted.

Sample success script for the on-prem deployment:

```
#!/appviewx/dependencies/appviewx_addons/Python/bin/python

print({"status":"AppResponseCode:0"})
```

Using Scripted Integrations for SaaS

1. Get the code-signed script from the AppViewX support team (help@appviewx.com). This will be a **.zip** file that includes the script and the signature.
2. Save the **.zip** file in all machines with the AppViewX Cloud Connector at the following location: **<CC_INSTALLATION_PATH>/deps/aps/**.
3. Mention in the **.zip** filename in all the relevant fields in the CERT+ user interface.

> **Note:** The folder path for the file is not required. Custom folder paths are restricted.

Sample success script for the SaaS deployment:

```
#!/usr/bin/python

print({"status":"AppResponseCode:0"})
```

Troubleshooting Script Usage Issues

Error	Cause	Resolution
File not found	The python path mentioned in the script file is not correct.	Check the path in the vendors pod or the mid-server-platform pod.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Error	Cause	Resolution
		For Python scripts: • Scripts for the on-prem deployment should start with `#!/appviewx/dependencies/appviewx_addons/Python/bin/python` • Scripts for the SaaS deployment should start with `#!/usr/bin/python`
...bin/python^M: bad interpreter	The `^M` is a carriage return character. Linux uses the line feed character to mark the end of a line, whereas Windows uses the two-character sequence CR LF. Your file has Windows line endings, which is confusing Linux	Remove the spurious CR characters and then code sign the script. You can remove these characters using the command: `sed -i -e 's/\r$//' scriptname.py`

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.

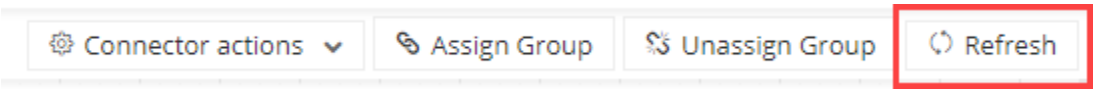
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Color Codes Status

The topological view follows a color codes scheme to identify certificate status.

Full list of color codes and their descriptions

Color	Description
Green	The certificate is available and valid.
Red	.The certificate has expired
Gray	Certificate push action failed.
Blue	The certificate will expire in 90 days.
Yellow	The certificate will expire in 30 days.
Orange	The certificate will expire in 10 days.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Full list of color codes and their descriptions (continued)

Color	Description
Black	The certificate has been revoked.
Mid Purple	The certificate associated with profiles is manually removed.

What's Next

After pushing a server certificate to a device, you can proceed with configuring expiry alerts:

- To set up expiry alerts and be notified of certificate statuses, see Configuring Expiry Alerts.

Pushing a Client Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Colour Codes Status

The topological view follows a colour codes scheme to identify certificate status.

Full list of color codes and their descriptions

Colour	Description
Green	The certificate is available and valid.
Red	The certificate has expired.
Gray	Certificate push action failed.
Blue	The certificate will expire in 90 days.
Yellow	The certificate will expire in 30 days.
Orange	The certificate will expire in 10 days.
Black	The certificate has been revoked.
Mid Purple	The certificate associated with profiles is manually removed.

Pushing an Intermediate Certificate to a Device

In the case of intermediate CA certificates or trust certificate renewal, the same should be pushed to the device in order to update the trust chain for the SSL communication. If this is not done, the SSL handshake will fail.

To push an intermediate certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Intermediate**.
   The **Intermediate Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. On the certificate topology page, click **Add Connector**.

4. Enter/select the **General Information** required for adding a connector.

Field descriptions for the General Information section

Field	Description
Category	Select the category from the dropdown list. The possible categories are: • ADC • Cloud • Firewall • MDM • Server • WAF.
Vendor	Select the desired vendor from the dropdown list.
Connector Name	Enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
Description	Enter the description in this field.

5. From the **SSL Template** section, to select a device listed under **Available devices**, click .
   The selected device is listed under the **Selected devices** list.

Pushing a Root Certificate to a Device

There can be renewal or change of root certificate in the trust store. In such occurrences, the user can push the root certificate to the desired endpoints to avoid the SSL handshake failure.

To push a root certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Root**.
   The **Root Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The certificate topology view is displayed.

3. On the certificate topology page, click **Add Connector**.

4. Enter the **General Information** required for adding a connector.

Field descriptions for the General Information section

Field	Description
Category	Select the category from the dropdown list. The possible categories are: • ADC • Cloud • Firewall • MDM • Server • WAF.
Vendor	Select the desired vendor from the dropdown list.
Connector Name	Enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
Description	Enter the description in this field.

5. From the **SSL Template** section, to select a device listed under **Available devices**, click .
The selected device is listed under the **Selected devices** list.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

For automating the certificate lifecycle management, in addition to enabling auto push of certificates, you can

- Enable auto regeneration of certificates.
- Enable auto renewal of certificates.
- Set alerts to be notified of all events and statuses of the certificates.

After automating the Auto Renew/Regenerate and enabling the Auto Push, you can proceed with configuring expiry alerts:

- To set up expiry alerts and be notified of certificate statuses, see Configuring Expiry Alerts.

Bulk Push for Intermediate/Root Certificates

Bulk push of the certificates can be triggered from the inventory by selecting more than one certificate. To push intermediate and root certificates in bulk:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Actions** > **Bulk Push**.
   The **Intermediate/Push Certificate** > **Add Connector** page is displayed.
2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	Select the required category from the dropdown list. The available options are: • **ADC** • **Server**.
***Vendor**	The **Vendor** field appears as follows based on the selected category: • By default, if the category is selected as **ADC**, the Vendor field will apear with **F5**. • By default, if the category is selected as **Server,** the Vendor field will apear with **LinuxServer**.
***Process Name**	For future reference, enter the process name (for example, **F5 bulk push**).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Allowed characters: • All alphanumeric characters (**a-z, A-Z, 0-9**) • All special characters **except** <, >, ", ;, and `
Description	Enter any additional details you want to record for this connector.

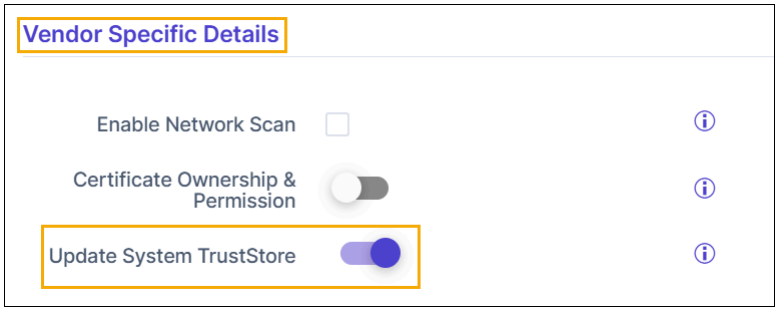
Based on the information entered here, the **SSL templates** section is populated with the list of available Linux Server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificates will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

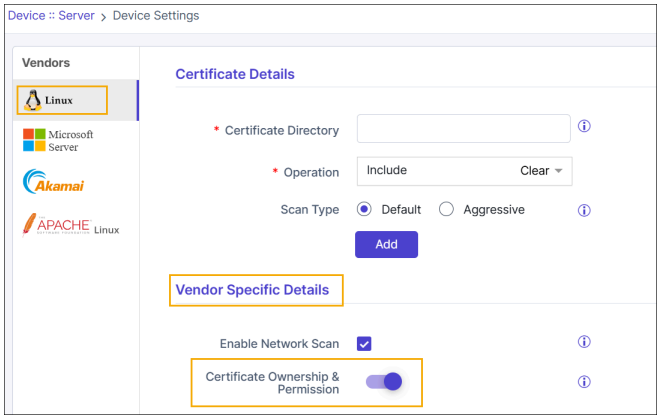
Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed. The supported certificate types are: • PEM (*.crt) • PEM (*.cer) • PEM (*.pem) • JKS (*.jks) • JKS (*.keystore) • PEM (Extensionless) • JKS (Extensionless).
Truststore Location	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the certificates to be pushed, is stored. **Note:** The alias names of JKS certificates in the truststore follow the format: <common name>_<thumbprint> of the certificate.
Truststore password	Enter the password required to access the truststore file for the JKS certificate to be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed for the JKS certificates.
Enable Truststore Update	This field is displayed for all **PEM** certificate types. Click the radio button to enable the Update System TrustStore option for root and intermediate certificates. **Note:** By default, this option is disabled. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** <⚙> **Vendor Specific Details** section > **Update System TrustStore**. 
Certificate Ownership & Permission	Enable the toggle button to customize the certificate ownership and define the file permissions for the certificates. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** <⚙> **Vendor Specific Details** section > **Certificate Ownership & Permission**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	 Field descriptions for the Certificate Ownership & Permission Details

Field descriptions for the Certificate Ownership & Permission Details

Field	Description
Owner	Enter the username for certificate ownership on the target device.
Owner Permission	Select the owner permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
User Group	Enter name of the user group that requires access to the certificate.
User Group Permission	Select the group permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
Other User Permission	Select the other user permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device.
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Reissuing Certificates

To update or modify its parameters, a certificate can be reissued by the same certificate authority that issued it. A common use case will be the addition of SAN names.

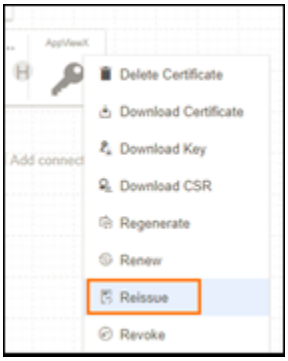
Note: Reissuing certificates will not be considered as a new order to the CA.

Note: You can reissue the certificates via the Certificate Inventory section also.

- Reissuing a Server Certificate
- Reissuing a Client Certificate

Reissuing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Reissue Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. To reissue a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Reissue**.



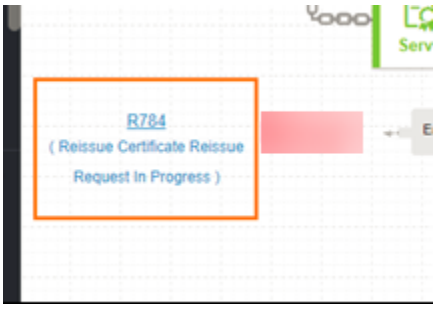
   The **Server Certificate** > **Reissue** page is displayed.

   On the **Server Certificate** > **Reissue** page, if required, you can edit the **Subject Alternate Names**. The **Key Type, Bit Length, Vendor Specific Details**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** can also be modified.

4. Click **Reissue**.
5. In the **Reissue** dialog box, enter the **Reason** for removal and any additional details as **Comments.**
6. Click **Yes**.

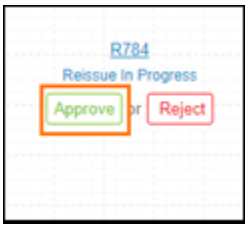
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The reissue process is initiated, as is displayed in the certificate topology view, alongside the connector



If the **Approval Required** checkbox is enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.

7. To approve the reissue request, from the certificate topology view, click **Approve**.



8. In the **Approve**dialog box, enter your **Comments**.
9. Click **Yes**.
10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. Click **Implement**.

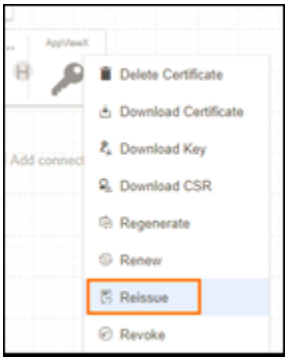
12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

After the certificate is reissued, the status updates to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Reissuing a Client Certificate

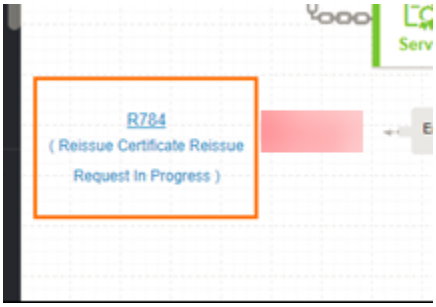
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Reissue Certificate** > **Client**.
   The **Client Certificate** page is displayed.
2. To reissue a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Reissue**.



   The **Client Certificate** > **Reissue** page is displayed.

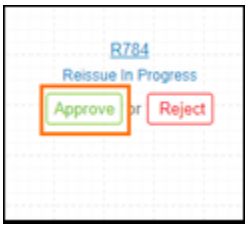
   On the **Client Certificate** > **Reissue** page, if required, you can edit the **Subject Alternate Names**. The **Key Type, Bit Length, Vendor Specific Details**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** can also be modified.

4. Click **Reissue**.
5. In the **Reissue** dialog box, enter the **Reason** for removal and any additional details as **Comments.**
6. Click **Yes**.
   The reissue process is initiated, as is displayed in the certificate topology view, alongside the connector

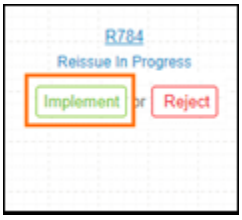


   If the **Approval Required** checkbox is enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.
7. To approve the reissue request, from the certificate topology view, click **Approve**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



8. In the **Approve**dialog box, enter your **Comments**.
9. Click **Yes**.
10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. Click **Implement**.



12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

    After the certificate is reissued, the status updates to **Completed**.

Revoking Certificates

Revocation is the process of making a certificate invalid. For example, you might need to revoke a certificate if the certificate is no longer required (or) certificate's private key is compromised. Make sure that you have permission to revoke a certificate and submit a request to the certificate authority. As soon as the certificate is revoked, it is not considered to be a trusted certificate. Revoked certificates are listed in the Certificate Revocation List (CRL) maintained by each certificate authority.

Important: Due to IDnomic API limitations, AppViewX is not notified when a certificate revocation request is declined. Hence, work orders for certificate revocation may still be shown as failing even if they are declined. This limitation will be addressed in the subsequent release versions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

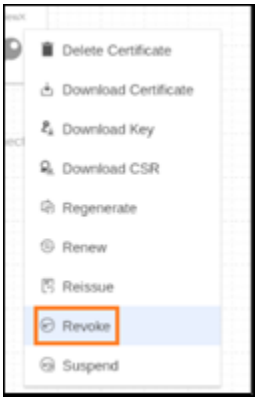
• Revoking a Server Certificate
• Revoking a Client Certificate
• Revoking a Device Certificate
• Revoking a Code Signing Certificate

Revoking a Server Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

Important: Due to IDnomic API limitations, AppViewX is not notified when a certificate revocation request is declined. Hence, work orders for certificate revocation may still be shown as failing even if they are declined. This limitation will be addressed in the subsequent release versions.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Server**.
   The **Server Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Revoke**.



   The **Certificate Revoke** dialog box is displayed.

4. **Note:** This step is applicable only for revoking DigiCert CA certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

In the **Certificate Revoke** dialog box, from the following options, select one to specify the certificate revoke **Type**:

- **Certificate**

  Selecting this option will only revoke the certificate that was selected from the inventory. On the DigiCert CA portal, the order status will remain **Active**.

- **Order ID**

  Selecting this option will display the **Order ID** field that is auto-populated with the order ID for the selected certificate.

  Revoking via this type will revoke all certificates belonging to this order ID.

5. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
6. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.

   If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.
7. On the certificate topology view, click **Approve** to proceed.

8. In the **Approve** dialog box, enter your **Comments**.
9. Click **Yes**.
10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. On the certificate topology view, click the **Implement** button to proceed.
12. In the **Implement** dialog box, enter your **Comments.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

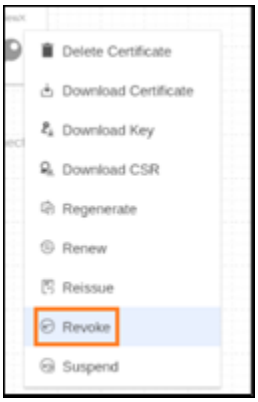
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    After the certificate is revoked, the status updates to **Completed**.

Revoking a Client Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

Important: Due to IDnomic API limitations, AppViewX is not notified when a certificate revocation request is declined. Hence, work orders for certificate revocation may still be shown as failing even if they are declined. This limitation will be addressed in the subsequent release versions.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Client**.
   The **Client Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Revoke**.



   The **Certificate Revoke** dialog box is displayed.

4. **Note:** This step is applicable only for revoking DigiCert CA certificates.

   In the **Certificate Revoke** dialog box, from the following options, select one to specify the certificate revoke **Type**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Certificate**

  Selecting this option will only revoke the certificate that was selected from the inventory. On the DigiCert CA portal, the order status will remain **Active**.

- **Order ID**

  Selecting this option will display the **Order ID** field that is auto-populated with the order ID for the selected certificate.

  Revoking via this type will revoke all certificates belonging to this order ID.

5. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
6. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.

   If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.
7. On the certificate topology view, click **Approve** to proceed.

8. In the **Approve** dialog box, enter your **Comments**.
9. Click **Yes**.
10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. Click **Implement**.
12. Click the **Implement** button to proceed.
13. In the **Implement** dialog box, enter your **Comments.**
14. Click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    After the certificate is revoked, the status updates to **Completed**.

Revoking a Device Certificate

> **Note:** For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Device**.
   The **Device Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Revoke**.
   The **Certificate Revoke** dialog box is displayed.
4. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
5. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.

   If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.
6. On the certificate topology view, click **Approve** to proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. In the **Approve** dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
10. Click **Implement**.
11. Click the **Implement** button to proceed.
12. In the **Implement** dialog box, enter your **Comments.**
13. Click **Yes**.
14. If the workflow request has to be approved automatically in the future, click **Schedule later**.

    After the certificate is revoked, the status updates to **Completed**.

Revoking a Code Signing Certificate

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

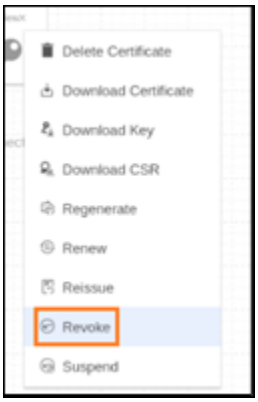
Important: Due to IDnomic API limitations, AppViewX is not notified when a certificate revocation request is declined. Hence, work orders for certificate revocation may still be shown as failing even if they are declined. This limitation will be addressed in the subsequent release versions.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revoke Certificate** > **Code Signing Certificate**.

   The **Code Signing Certificate** page is displayed.
2. To revoke a certificate,under **Common Name**, select the required certificate name.

   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Revoke**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



The **Certificate Revoke** dialog box is displayed.

4. **Note:** This step is applicable only for revoking DigiCert CA certificates.

   In the **Certificate Revoke** dialog box, from the following options, select one to specify the certificate revoke **Type**:

   - **Certificate**

     Selecting this option will only revoke the certificate that was selected from the inventory. On the DigiCert CA portal, the order status will remain **Active**.

   - **Order ID**

     Selecting this option will display the **Order ID** field that is auto-populated with the order ID for the selected certificate.

     Revoking via this type will revoke all certificates belonging to this order ID.

5. In the **Certificate Revoke** dialog box, from the dropdown list, select the reason for revoking the certificate.
6. Enter your comments in the **Comments** text field (optional) and click **Yes**.
   The revoke process is initiated for the selected certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the **Approval Required** checkbox was enabled on the **Certificate Policy** page, the request goes to the **Approve** and **Implementation** stages.

7. On the certificate topology view, click **Approve** to proceed.

8. In the **Approve** dialog box, enter your **Comments**.
9. Click **Yes**.
10. If the workflow request has to be approved automatically in the future, click **Schedule later**.
11. Click **Implement**.
12. Click the **Implement** button to proceed.
13. In the **Implement** dialog box, enter your **Comments.**
14. Click **Yes**.
15. If the workflow request has to be approved automatically in the future, click **Schedule later**.

After the certificate is revoked, the status updates to **Completed**.

Regenerating Certificates

Important: The **Regenerate Certificate** CLM action is displayed in the CERT+ menu only for authorized user roles. For more context, refer to the Configuring Role and Resource-Based Access Control and Creating a Role sections in the Platform User Guide.

Certificate regeneration allows you to create a new certificate with the same parameters as an existing certificate. Certificate regeneration will be a new order to the Certificate authority. This will come in handy if the user wants to switch the CA for a certificate.

- Regenerating a Server Certificate
- Regenerating a Client Certificate
- Regenerating a Code Signing Certificate
- Tracking Certificate Regeneration via the Process Explorer
- Enabling Auto Regeneration for Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

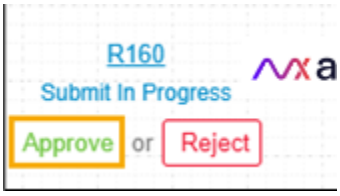
Regenerating a Server Certificate

Important: The **Regenerate Certificate** CLM action is displayed only for authorized user roles. For more context, refer to the **Configuring Role and Resource-Based Access Control** and **Creating a Role** sections in the Platform User Guide.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. To regenerate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Regenerate**.
   The **Server Certificate > Regenerate** page is displayed.
4. On the **Server Certificate > Regenerate** page, modify the required details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** sections.

   Note: For field descriptions, you can refer to the instructions for enrolling a server certificate.

5. Click **Regenerate**.
   The regenerate process is initiated.
6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve** dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
   a. Select the **Implementation Time** from the calendar field.
   b. Enter the comments in the field.
   c. Click **Yes**.
   The approval process is initiated.
10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    a. Select the **Implementation Time** from the calendar field.
    b. Enter the comments in the field.
    c. Click **Yes**.

    After the certificate regeneration is complete, the status updates to **Completed**.

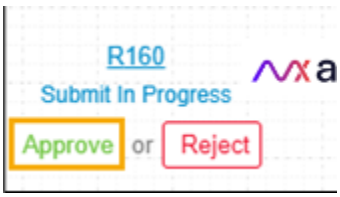
Regenerating a Client Certificate

Important: The **Regenerate Certificate** CLM action is displayed only for authorized user roles. For more context, refer to the **Configuring Role and Resource-Based Access Control** and **Creating a Role** sections in the Platform User Guide.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. To regenerate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Regenerate**.
   The **Client Certificate > Regenerate** page is displayed.
4. On the **Client Certificate > Regenerate** page, modify the required details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** sections.

   Note: For instructions on entering inputs in the above sections, click here.

5. Click **Regenerate**.
   The regenerate process is initiated.
6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve** dialog box, enter your **Comments**.
8. Click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
   a. Select the **Implementation Time** from the calendar field.
   b. Enter the comments in the field.
   c. Click **Yes**.

   The approval process is initiated.
10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**
12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    a. Select the **Implementation Time** from the calendar field.
    b. Enter the comments in the field.
    c. Click **Yes**.

    After the certificate regeneration is complete, the status updates to **Completed**.

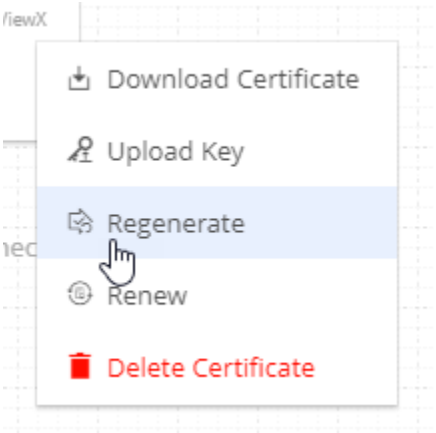
Regenerating a Code Signing Certificate

> **Important:** The **Regenerate Certificate** CLM action is displayed only for authorized user roles. For more context, refer to the **Configuring Role and Resource-Based Access Control** and **Creating a Role** sections in the Platform User Guide.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.

   The **Code Signing Certificate** page is displayed.
2. To regenerate a certificate, under **Common Name**, select the required certificate name.

   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Regenerate**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Code Signing Certificate > Regenerate** page is displayed.

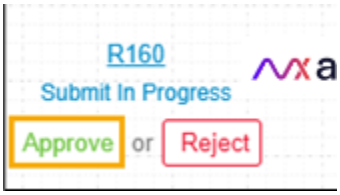
4. On the **Code Signing Certificate > Regenerate** page, modify the required details in the **General Information**, **CA Details**, **CSR Parameters**, **Attachments**, **Generic Fields**, **Vendor-Specific Details**, and **Custom Attributes** sections.

> **Note:** For instructions on entering inputs in the above sections, click here.

5. Click **Regenerate**.

   The regenerate process is initiated.

6. On the certificate topology view, click **Approve** to proceed.



7. In the **Approve** dialog box, enter your **Comments**.
8. Click **Yes**.
9. If the workflow request has to be approved automatically in the future, click **Schedule later**.
   a. Select the **Implementation Time** from the calendar field.
   b. Enter the comments in the field.
   c. Click **Yes**.

   The approval process is initiated.

10. On the certificate topology view, click the **Implement** button to proceed.
11. In the **Implement** dialog box, enter your **Comments.**
12. Click **Yes**.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
    a. Select the **Implementation Time** from the calendar field.
    b. Enter the comments in the field.
    c. Click **Yes**.

    After the certificate regeneration is complete, the status updates to **Completed**.

Tracking Certificate Regeneration via the Process Explorer

The **Process Explorer** is a listing of all certificates scheduled for regeneration on present day and certificates awaiting approval for regeneration. Once a certificate is regenerated, it is removed from this listing. The **Process Explorer** is useful for monitoring the regeneration status.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To access the process explorer:

Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Regenerate Certificate** > **Process Explorer**.

Important: The **Regenerate Certificate** CLM action is displayed in the CERT+ menu only for authorized user roles. For more context, refer to the **Configuring Role and Resource-Based Access Control** and **Creating a Role** sections in the Platform User Guide.

The **Regenerate Certificate** page with the listings is displayed.

Enabling Auto Regeneration for Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The certificate details are displayed.

5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

What's Next?

For automating the certificate lifecycle management, in addition to auto regeneration, you can:

- Enable auto renewal of certificates.
- Enable auto push of certificates to endpoints. To do this, add an application connector to push the certificate to an AWS device and select the **Push Automatically** checkbox.
- Set alerts to be notified of all events and statuses of the certificates.

Reinstating Certificates

Reinstate is an action that can be applied only on the suspended certificate. Suspend is a temporary revocation of a certificate where the user is unsure about certificate usage. Once reinstated, the certificate will get resumed to serve its purpose normally. The suspend and reinstate are the actions supported only by a few CAs such as Microsoft, Entrust, and so on.

> **Note:** Only the certificates issued by the Microsoft and EJBCA certificate authorities can be reissued.

- Reinstating a Server Certificate
- Reinstating Client Certificate
- Reinstating Code Signing Certificate

Reinstating a Server Certificate

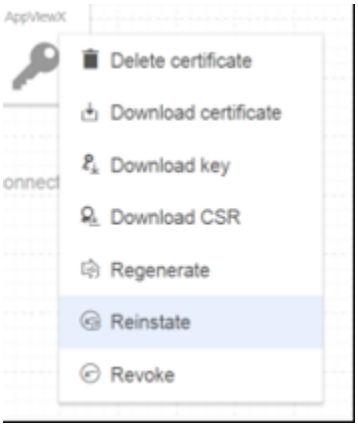
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. To reinstate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Reinstate**.
   The **Certificate Reinstate** dialog box is displayed.
4. In the **Certificate Reinstate** dialog box, from the dropdown list, select a reason for reinstating the certificate.
5. Enter you **Comments** in the text field and click **Yes**.

Reinstating Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. To reinstate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Reinstate**.



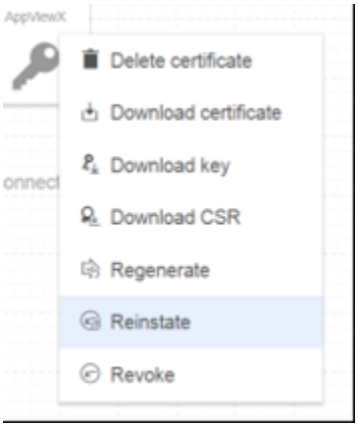
   The **Certificate Reinstate** dialog box is displayed.
4. In the **Certificate Reinstate** dialog box, from the dropdown list, select a reason for reinstating the certificate.
5. Enter you **Comments** in the text field and click **Yes**.

Reinstating Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. To reinstate a certificate,under **Common Name**, select the required certificate name.
   The certificate topology view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Reinstate**.



   The **Certificate Reinstate** dialog box is displayed.
4. In the **Certificate Reinstate** dialog box, from the dropdown list, select a reason for reinstating the certificate.
5. Enter you **Comments** in the text field and click **Yes**.

Duplicating Certificates

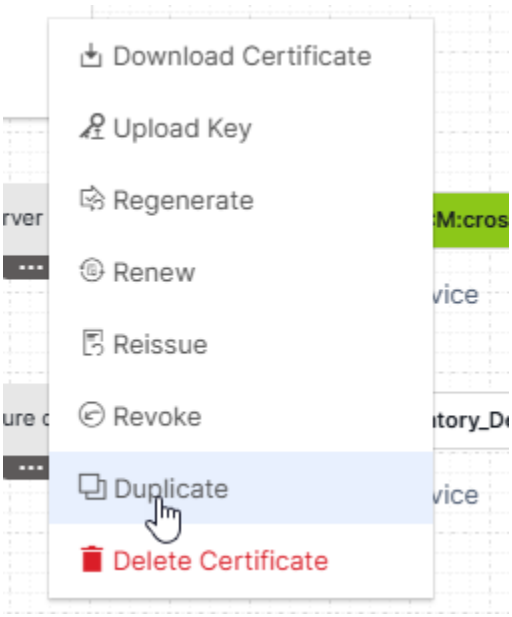
Certificate duplication refers to the process of creating a copy of an existing certificate while maintaining its original attributes and key usage information. This action is typically used when a new certificate with similar properties is required for a different application or system without altering or renewing the original certificate.

Important: Currently, this feature is supported for only DigiCert certificates. For the full list of DigiCert certificate types that can be duplicated, click here.

To duplicate a certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. To open the holistic view of a certificate, under **Common Name**, select the required certificate name.
3. From the **(More)** menu for the certificate, click **Duplicate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



The **Server Certificate > Duplicate** page is displayed for the selected certificate.

For duplicating a certificate:

- The uneditable fields are displayed, which means these are attributes you cannot change for a duplicate certificate.

  For field descriptions of the editable fields, click here.
- While the common name for the duplicate certificate can be updated, it is valid only if it conforms with the SAN/DNS selected for the parent certificate.
- A duplicate certificate can only be:
  - Downloaded
  - Duplicated
  - Revoked (at the certificate level as well as at the order level)

4. Click **Duplicate**.
   The message **Cert duplicate triggered successfully** is displayed.

   You will be redirected to the holistic view of the certificate.
5. Refresh to view the certificate in the holistic view and the certificate inventory.

DigiCert CA Certificate Types Supported for Duplication

Currently, only the following DigiCert CA certificate types can be duplicated:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Secure Site OV
- Secure Site EV
- Secure Site EV SSL
- Secure Site EV Multi-Domain SSL
- Basic OV
- Basic EV
- Multi-Domain SSL
- Wildcard
- EV SSL
- EV Multi-Domain
- GeoTrust TrueBusiness ID EV
- GeoTrust TrueBusiness ID OV
- Thawte SSL Webserver EV
- Thawte SSL Webserver OV
- Private Multi-Domain SSL
- Private SSL Wildcard
- Private SSL OV

Running Revocation Check-OCSP

A sophisticated method of detecting revoked certificates is the Online Certificate Status Protocol (OCSP). Instead of downloading and parsing the entire CRL, the client can send the certificate in question to the CA. And then, the CA replies status of the certificate is good, revoked, or unknown. This method involves far less overhead than CRL and is also more reliable.

- Running Revocation Check for Server Certificate
- Running Revocation Check for Client Certificate
- Running Revocation Check for Device Certificate
- Running Revocation Check for Code Signing Certificate

Running Revocation Check for Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Server**. The **Server Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Tip:** You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

   Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

   The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Running Revocation Check for Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Client**.
   The **Client Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

> **Tip:** You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

   Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

   The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Running Revocation Check for Device Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Device**.
   The **Server Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

   Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

   The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Running Revocation Check for Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Revocation Check - OCSP** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **Revocation Check**.
   The **Revocation Check** dialog box is displayed.
4. To perform revocation validation, in the **Revocation Check** dialog box, click **OK**.
   Revocation check for the selected certificate(s) will be initiated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Once the revocation has been validated, the color code (displayed along with the **Common name** of the certificate) will be updated.

The status of the revoked certificate is displayed in the **Valid to (GMT)** column.

Generating Certificate Signing Request (CSR)

CERT+ can be used as a CSR generation tool where you can choose either the keys that can be generated in the filesystem or any HSM device integrated with AppViewX. CSR, or Certificate Signing Request, consists of requester info in a standardized way. Based on an organization's needs and the business model, the CSR generation and approval flow can be customized.

- Generating Manual CSR for Server Certificate
- Generating Manual CSR for Code Signing Certificate

Generating Manual CSR for Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Generate CSR** > **Server**.
   The **Generate CSR : Server** page is displayed.
2. In the **Group details** section, from the **Assign Group** dropdown list, select the group of certificates you want to assign the CSR to.
3. Enter the **CSR details**.

Field descriptions for the CSR details section

Option	Description
***CSR Selection**	Select the key generation of CSR as required. The possible selections are: • AppViewX • HSM
***Device Type**	Select the type of device as required: Options are: • **HSM Devices** • **ADC Devices**
***Device**	Select the device from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Option	Description
***Key Handler Name**	Enter the name of the key handler.
***Key Reference Name**	Enter the name of the key reference.
***Common Name**	Name that is to be present in the certificate. **Note:** No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter the alternative subject name. For example, DNS or IP address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property window from the holistic view.
***Organization**	The Organization name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The Organization Unit name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The Locality name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The State name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	The Country name that is to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a two-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in **Days**, **Months**, and **Years** from the dropdown lists.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Option	Description
Challenge Password	The challenge password for the certificate. Enter if it is applicable. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	The password to confirm the Challenge Password entered and match with the Challenge Password.
***Hash Function**	The Hash function with which the CSR has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

4. In the **Attachments** section, upload any attachments relevant to the CSR generation process.

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the **Upload** button to select the file.
Note: Maintains if there are any additional documents to be maintained in AppViewX. These documents will not be submitted to CA. It is a non-mandatory section.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Tip: You can use **the Search** option to find the attachments from the attachment list.

5. To generate the CSR and add it to the intended group, click **Add**.

Generating Manual CSR for Code Signing Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Generate CSR** > **Code Signing Certificate**.
   The **Generate CSR : Code Signing** page is displayed.
2. In the **Group details** section, from the **Assign Group** dropdown list, select the group of certificates you want to assign the CSR to.
3. Enter the **CSR details**.

Field descriptions for the CSR details section

Option	Description
***CSR Selection**	Select the key generation of CSR as required. The possible selections are: • AppViewX • HSM.
***Device Type**	Select the type of device as required: Options are: • **HSM Devices** • **ADC Devices.**
***Device**	Select the device from the dropdown list.
***Key Handler Name**	Enter the name of the key handler.
***Key Reference Name**	Enter the name of the key reference.
***Common Name**	Name that is to be present in the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Option	Description
	Note: No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	Enter the alternative subject name. For example, DNS or IP address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property window from the holistic view.
***Organization**	The Organization name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	The Organization Unit name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The Locality name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The State name that to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	The Country name that is to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a two-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in **Days**, **Months**, and **Years** from the dropdown lists.
Challenge Password	The challenge password for the certificate. Enter if it is applicable. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	The password to confirm the Challenge Password entered and match with the Challenge Password.
***Hash Function**	The Hash function with which the CSR has to be signed. For Microsoft Enterprise CA, the targeted CA decides the hash function while issuing the certificate. This field

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Option	Description
	will be auto-filled and editable based on the configuration in the selected group's policy.
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

4. In the **Attachments** section, upload any attachments relevant to the CSR generation process.

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the **Upload** button to select the file.
Note: Maintains if there are any additional documents to be maintained in AppViewX. These documents will not be submitted to CA. It is a non-mandatory section.	

Tip: You can use **the Search** option to find the attachments from the attachment list.

5. To generate the CSR and add it to the intended group, click **Add**.

Migrating CAs (CA Switch)

The CA Switch feature in the **Inventory** module allows you to re-enroll certificates from one CA to another CA. Once triggered, the certificate migration readiness for every certificate will be shown in the **Process Explorer**, which needs to be validated before the CA switch is performed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Migrating the CA for Server Certificate
• Migrating the CA for Client Certificate
• Migrating the CA for Code Signing Certificates

Migrating the CA for Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Server**.
   The **Server Certificate** page is displayed.
2. To run the revocation check for a certificate, under **Common Name**, select the checkbox corresponding to the required certificate.

> **Tip:** You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.

Field descriptions for the CA Switch details

Options	Description
***Target CA**	From the dropdown list, select the target CA for the CA switch operation.
***Settings**	From the dropdown list, select the CA setting that will be applied to the CA switch operation.
***Name**	Enter a unique name for the CA switch operation. This will help to identify the CA switch process within the system. **Constraints**: • Valid special characters for CA switch name: space, **.**, **-**, _ • CA switch name cannot start with a special character.

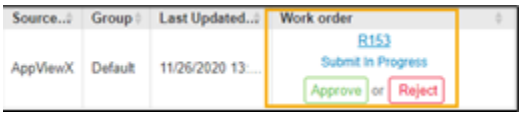
5. Click **Save**.
   The **CA Switch Summary** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Understanding the CA Switch Summary

Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

6. For the certificate you want to migrate, select the corresponding checkbox.
7. In the **Common Name** column, click the eye icon to view certificate details.
8. In the **CSR details** column, click **Update CSR** to review the details.
9. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
10. Click **Submit**.
11. Perform the required actions in the Work order column.



12. In the **Work order** column, click **Approve**.
    The **Approve**dialog box is displayed.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
14. Select the **Implementation Time** from the calendar field.
15. Enter the **Comments**.
16. Click **Yes**.
17. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

18. In the **Work order** column, click **Implement**.
    The **Implement** dialog box appears.
19. If the workflow request has to be approved automatically in the future, click **Schedule later**.
20. Select the **Implementation Time** from the calendar field.
21. Enter the **Comments** in the field.
22. Click **Yes**.
23. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
24. Click the refresh icon on the top-right of the page to update the Work Order status.
    After the CA Switch is completed, the Work order status changes to **Completed**.

Bulk Migrating the CA for Server Certificates

Important: Currently, the bulk CA switch feature has been enabled only for switching from:

- All CAs to Microsoft CA (Enterprise and Standalone)
- Microsoft CA (Enterprise and Standalone) to Microsoft CA (Enterprise and Standalone)

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Server**.
   The **Server Certificate > Server Certificate** page is displayed.
2. Select the checkboxes corresponding to the certificates for which the CA has to be migrated.
3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.

Field descriptions for the CA Switch details

Options	Description
***Target CA**	From the dropdown list, select **Microsoft Enterprise CA**/**Microsoft Standalone CA**.
***Settings**	From the dropdown list, select the CA setting that will be applied to the CA switch operation.
***Name**	Enter a unique name for the CA switch operation. This will help to identify the CA switch process within the system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
	Constraints: • Valid special characters for CA switch name: space, **.**, **-**, _ • CA switch name cannot start with a special character.

5. Click **Save**.
   The **CA Switch Summary** page is displayed.

   This page lists all the CA switch requests pending approval.
6. To bulk approve CA switch requests, select the checkboxes corresponding to the required requests.
   The **Bulk Update CSR** and **Actions** buttons are enabled.
7. Click **Bulk Update CSR**.
   The **Update Connector Details** dialog box is displayed.
8. Update the connector details, as required.
9. Click **Update**.
   You will be redirected to the CA switch summary page. The **Certificate Status** is updated to **Ready to migrate**.
10. Select the required CA switch requests.
11. Click **Submit**.
    The message **Selected certificates have been submitted.** is displayed.

    Work order details of the selected requests are updated to display the work order number, and the **Approve** and **Reject** buttons.
12. Select the required CA switch requests.
13. To approve the CA switch request, from the **Actions** menu, select **Proceed Further**.
14. In the **Confirmation** dialog box displayed, click **Yes**.
15. To implement the CA switch requests, from the **Actions** menu, again, select **Proceed Further**.
16. In the **Confirmation** dialog box displayed, click **Yes**.
17. Once the CA switch requests are processed, the **Work Order status** is updated to **Completed**.

Migrating the CA for Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Client**.
   The **Client Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.

3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.

Field descriptions for the CA Switch details

Options	Description
***Target CA**	From the dropdown list, select the target CA for the CA switch operation.
***Settings**	From the dropdown list, select the CA setting that will be applied to the CA switch operation.
***Name**	Enter a unique name for the CA switch operation. This will help to identify the CA switch process within the system. **Constraints**: • Valid special characters for CA switch name: space, **.**, **-**, _ • CA switch name cannot start with a special character.

5. Click **Save**.
   The **CA Switch Summary** page is displayed.

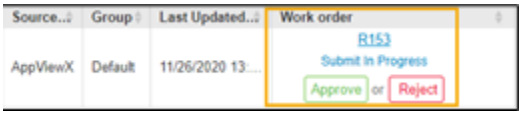
Understanding the CA Switch Summary

Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options	Description
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

6. For the certificate you want to migrate, select the corresponding checkbox.
7. In the **Common Name** column, click the eye icon to view certificate details.
8. In the **CSR details** column, click **Update CSR** to review the details.
9. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
10. Click **Submit**.
11. Perform the required actions in the Work order column.



12. In the **Work order** column, click **Approve**.
    The **Approve**dialog box is displayed.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
14. Select the **Implementation Time** from the calendar field.
15. Enter the **Comments**.
16. Click **Yes**.
17. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
18. In the **Work order** column, click **Implement**.
    The **Implement** dialog box appears.
19. If the workflow request has to be approved automatically in the future, click **Schedule later**.
20. Select the **Implementation Time** from the calendar field.
21. Enter the **Comments** in the field.
22. Click **Yes**.
23. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

24. Click the refresh icon on the top-right of the page to update the Work Order status.
    After the CA Switch is completed, the Work order status changes to **Completed**.

Bulk Migrating the CA for Client Certificates

Important: Currently, the bulk CA switch feature has been enabled only for switching from:

- All CAs to Microsoft CA (Enterprise and Standalone)
- Microsoft CA (Enterprise and Standalone) to Microsoft CA (Enterprise and Standalone)

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Client**.
   The **Client Certificate** page is displayed.
2. Select the checkboxes corresponding to the certificates for which the CA has to be migrated.
3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.

Field descriptions for the CA Switch details

Options	Description
***Target CA**	From the dropdown list, select **Microsoft Enterprise CA**/**Microsoft Standalone CA**.
***Settings**	From the dropdown list, select the CA setting that will be applied to the CA switch operation.
***Name**	Enter a unique name for the CA switch operation. This will help to identify the CA switch process within the system. **Constraints**: • Valid special characters for CA switch name: space, **.**, **-**, _ • CA switch name cannot start with a special character.

5. Click **Save**.
   The **CA Switch Summary** page is displayed.

   This page lists all the CA switch requests pending approval.
6. To bulk approve CA switch requests, select the checkboxes corresponding to the required requests.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Bulk Update CSR** and **Actions** buttons are enabled.

7. Click **Bulk Update CSR**.
   The **Update Connector Details** dialog box is displayed.
8. Update the connector details, as required.
9. Click **Update**.
   You will be redirected to the CA switch summary page. The **Certificate Status** is updated to **Ready to migrate**.
10. Select the required CA switch requests.
11. Click **Submit**.
    The message **Selected certificates have been submitted.** is displayed.

    Work order details of the selected requests are updated to display the work order number, and the **Approve** and **Reject** buttons.
12. Select the required CA switch requests.
13. To approve the CA switch request, from the **Actions** menu, select **Proceed Further**.
14. In the **Confirmation** dialog box displayed, click **Yes**.
15. To implement the CA switch requests, from the **Actions** menu, again, select **Proceed Further**.
16. In the **Confirmation** dialog box displayed, click **Yes**.
17. Once the CA switch requests are processed, the **Work Order status** is updated to **Completed**.

Migrating the CA for Code Signing Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Code Signing**.
   The **Code Signing Certificate** page is displayed.
2. To run the revocation check for a certificate,under **Common Name**, select the checkbox corresponding to the required certificate.

   Tip: You can run the revocation check for more than one certificate at the same time. To do this, select the checkboxes corresponding to all the required certificates.
3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Switch details

Options	Description
***Target CA**	From the dropdown list, select the target CA for the CA switch operation.
***Settings**	From the dropdown list, select the CA setting that will be applied to the CA switch operation.
***Name**	Enter a unique name for the CA switch operation. This will help to identify the CA switch process within the system. **Constraints**: • Valid special characters for CA switch name: space, **.**, **-**, _ • CA switch name cannot start with a special character.

5. Click **Save**.

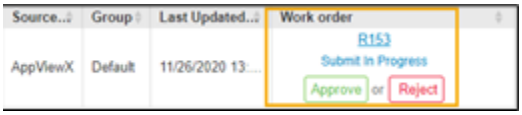
   The **CA Switch Summary** page is displayed.

Understanding the CA Switch Summary

Options	Description
	Allows you to delete the certificates from the list if decided not to migrate.
	Refreshes the CA Switch summary page.
	Displays the number of certificates displayed on the current page.
	Allows you to move to the next and previous page if more pages exist.
Search	Searches for the given keyword in the field and results in the feature that matches the search keyword.
Color Coding Status	The color code on the top-right indicates the status of the certificate on the CA Switch summary page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. For the certificate you want to migrate, select the corresponding checkbox.
7. In the **Common Name** column, click the eye icon to view certificate details.
8. In the **CSR details** column, click **Update CSR** to review the details.
9. In the **Validation log** column, click **View** to display the events recorded during the CA switch.
10. Click **Submit**.
11. Perform the required actions in the Work order column.



12. In the **Work order** column, click **Approve**.
    The **Approve** dialog box is displayed.
13. If the workflow request has to be approved automatically in the future, click **Schedule later**.
14. Select the **Implementation Time** from the calendar field.
15. Enter the **Comments**.
16. Click **Yes**.
17. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
18. In the **Work order** column, click **Implement**.
    The **Implement** dialog box appears.
19. If the workflow request has to be approved automatically in the future, click **Schedule later**.
20. Select the **Implementation Time** from the calendar field.
21. Enter the **Comments** in the field.
22. Click **Yes**.
23. In the **Work order** column, click the status if you want to see the **Summary** and **Details** of the progress.
    The **View Work order Status** page is displayed.
24. Click the refresh icon on the top-right of the page to update the Work Order status.
    After the CA Switch is completed, the Work order status changes to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Bulk Migrating the CA for Code Signing Certificates

Important: Currently, the bulk CA switch feature has been enabled only for switching from:

- All CAs to Microsoft CA (Enterprise and Standalone)
- Microsoft CA (Enterprise and Standalone) to Microsoft CA (Enterprise and Standalone)

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **CA Switch** > **Code Signing**.
   The **Code Signing Certificate** page is displayed.
2. Select the checkboxes corresponding to the certificates for which the CA has to be migrated.
3. From the **Actions** menu, select **CA Switch**.
   The **CA Switch** dialog box is displayed.
4. Enter/Select the switch-related details.

Field descriptions for the CA Switch details

Options	Description
***Target CA**	From the dropdown list, select **Microsoft Enterprise CA**/**Microsoft Standalone CA**.
***Settings**	From the dropdown list, select the CA setting that will be applied to the CA switch operation.
***Name**	Enter a unique name for the CA switch operation. This will help to identify the CA switch process within the system. **Constraints**: • Valid special characters for CA switch name: space, **.**, **-**, _ • CA switch name cannot start with a special character.

5. Click **Save**.
   The **CA Switch Summary** page is displayed.

   This page lists all the CA switch requests pending approval.
6. To bulk approve CA switch requests, select the checkboxes corresponding to the required requests.
   The **Bulk Update CSR** and **Actions** buttons are enabled.
7. Click **Bulk Update CSR**.
   The **Update Connector Details** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. Update the connector details, as required.
9. Click **Update**.
   You will be redirected to the CA switch summary page. The **Certificate Status** is updated to **Ready to migrate**.
10. Select the required CA switch requests.
11. Click **Submit**.
    The message **Selected certificates have been submitted.** is displayed.

    Work order details of the selected requests are updated to display the work order number, and the **Approve** and **Reject** buttons.
12. Select the required CA switch requests.
13. To approve the CA switch request, from the **Actions** menu, select **Proceed Further**.
14. In the **Confirmation** dialog box displayed, click **Yes**.
15. To implement the CA switch requests, from the **Actions** menu, again, select **Proceed Further**.
16. In the **Confirmation** dialog box displayed, click **Yes**.
17. Once the CA switch requests are processed, the **Work Order status** is updated to **Completed**.

Running the SSL Checker for a Certificate

SSL certificate deployment can be validated using the SSL checker feature in AppViewX. This validates the SSL certificate deployment, trustchain, ciphersuites, and supported TLS versions for a given service endpoint.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **SSL Checker**.
   The **SSL Checker** page is displayed.
2. Enter the **FQDN** and **IP address** details.
3. Click **Add**.
4. To run the SSL checker, click **Validate**.

Managing the Certificate Inventory

Note: The CERT+ certificate inventory is updated periodically. If you are looking for real-time updates, please refer to the documentation for CERT+ Insights.

The certificate inventory allows you to take inventory of, and proactively manage all your certificates. This will be a single source of truth for all the certificates in the organization. Every certificate action can be performed from the inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Take inventory of all your digital certificates
- Keeps you informed of impending expirations
- Creates certificate tasks via workflows to renew expiring certificates
- Creates incidents for already expired certificates
- Prioritizes certificate importance
- Helps you proactively manage your certificates
- Helps you avoid manually tracking a large volume of certificates
- Prevents security breaches due to expired or expiring certificates

In the Certificate Inventory section, you can:

- enroll a certificate
- renew a certificate
- push to device
- reissue a certificate
- revoke a certificate
- regenerate a certificate
- reinstate a certificate
- revocation check
- upload a certificate
- download a certificate.

- Managing the Server Certificate Inventory
- Managing the Client Certificate Inventory
- Managing the Code Signing Certificate Inventory
- Managing the Device Certificate Inventory
- Managing the Intermediate Certificate Inventory
- Managing the Root Certificate Inventory
- Uploading a Certificate
- Downloading Certificates
- Archiving Certificates

Managing the Server Certificate Inventory

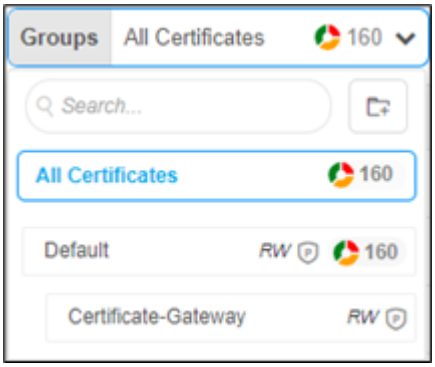
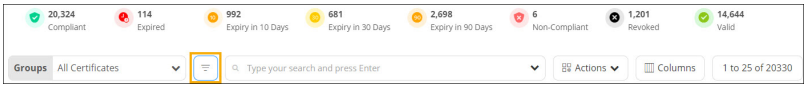
Server certificate inventory is where all the server certificates with the EKU (Extended Key Usage) Server and Client authentication will be present. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

or many certificates and perform bulk certificate renewal, bulk certificates CA migration, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

On the **Certificate Inventory** > **Server** certificate page, all the server certificates are listed. You can perform the following actions:

Options available on the Server Certificate inventory page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates. 
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates The following certificate actions are supported:
Columns	Allows you to select the columns to be displayed on the Server Certificate inventory page **Note:** In the current implementation, the **Certificate Type** column is populated for only selected CAs. To populate it for the SwissSign CA, see the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options available on the Server Certificate inventory page (continued)

Options	Description
Toggle	Allows you to toggle between the following display options for the Server Certificate inventory: • **Reports**: Displays reports related to server certificates. For more information, click here. • **List**: Displays the list of server certificates.

The list of actions you can perform on the certificates are:

- Export Certificates - To export the server certificate.
- Download Certificates - To download a certificate from an inventory to a file (the private key, root, and intermediate certificates can be included in the download.
- Delete - To delete the server certificate.
- Change Status - To change the server certificate status.
- Assign Group - To assign a group to the certificate.
- Unassign Group - To unassign a group from the certificate.
- Add/Modify Comments - To add/modify comments to the certificate.
- Certificate Attributes - To update the certificate attributes.
- Bulk Update Attributes Value - To update the certificate attributes for certificates.
- Renew Certificates - To renew certificates before expiry.
- Revoke Certificates - To revoke certificates
- CA Switch - Switching to another Certificate Authority (CA) for your SSL needs.
- Revocation Check - To check the revocation status of the certificate.

Populating the Certificate Type Column for the SwissSign CA

In the current implementation, for the SwissSign CA, the certificate type column is not auto populated on display. To populate it:

1. Run the Certificate Authority discovery scan for SwissSign CA.
2. For the discovered certificates, manually modify the status to **Managed** or **Monitored**.

   The certificate type for each SwissSign certificate is added to the column.

   The data is additionally leveraged to generate reports for SwissSign CA, categorized by certificate type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

Once you have discovered certificates, you are ready to proceed with any of the following certificate actions:

- If you want to Auto Renew the Discovered Certificate.
- If you want to Auto Regenerate the Discovered Certificate.
- Exporting a Server Certificate
- Adding/Modifying Comments for Server Certificates
- Editing Server Certificate Details via the Connector
- Deleting Server Certificates
- Changing Server Certificate Status
- Assigning Certificate Group for Server Certificates
- Unassigning Certificate Group from Server Certificates
- Bulk Revoking Server Certificates
- Updating Certificate Attributes for Server Certificates
- Bulk Updating Certificate Attributes

Exporting a Server Certificate

You can export certificate(s) from the Server Certificate inventory in the form of columns and values. These certificates can be exported either in an **.xls** or **.csv** format. This can be used for reporting or making another inventory.

To export a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** pop-up window is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Adding/Modifying Comments for Server Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, select the certificate that you want to revoke.
3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** dialog box that is displayed, enter a comment and click **Save**.

Editing Server Certificate Details via the Connector

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Open the holistic view of the certificate you want to edit.
3. In the holistic view, hover over the connector you want to edit.
4. From the menu displayed, click **Edit**.
   The **Server certificate > <certificate name>** page is displayed.
5. Edit the certificate details as required.
   For field descriptions and instructions see Enrolling a Server Certificate.

Deleting Server Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any reports and alerts.

Deleting Individual Server Certificates from the Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Server Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.

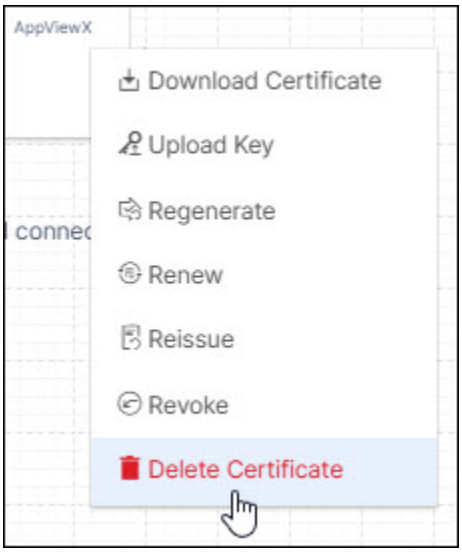
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

Deleting Individual Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Server Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) icon and from the menu displayed, click **Delete Certificate**.

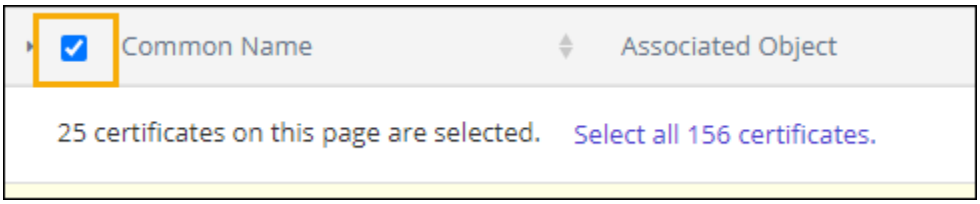


4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The server certificate is deleted from the AppViewX inventory.

Deleting all Server Certificates

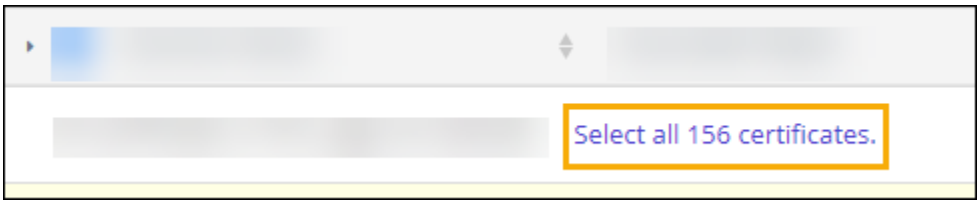
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. In the **Server Certificate** inventory, select the checkbox next to the **Common Name** field label.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

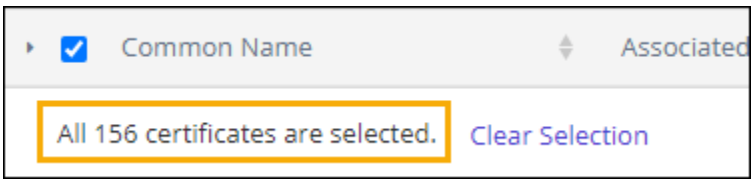


All certificates on the current page are selected.

3. To select all certificates in the server certificate inventory, click **Select all <no. of certificates> certificates**.



This will select all certificates across all pages in the server certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   All certificates in the server certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificates will be deselected.

Changing Server Certificate Status

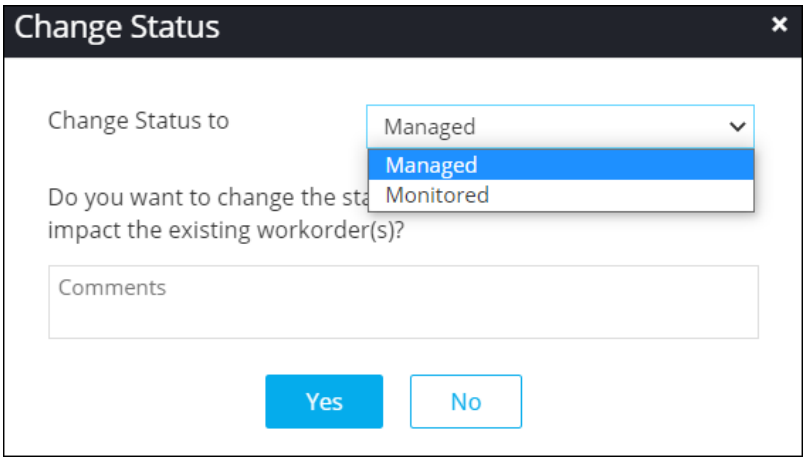
The status of a certificate can be set as monitored or managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, you can only view the certificate details in reports and in the inventory. When the certificates are set as

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Managed, the certificate-related actions along with push/bind operations can be performed along with viewing of the certificates in the reports and inventory.

To change the server certificate status:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the certificate for which you want to change the status.
3. From the **Actions** dropdown, click **Change Status**.
4. In the **Change Status** pop-up window that is displayed, in the **Change Status to** field, select the status of the certificate field as **Managed** or **Monitored**.



5. Enter the reason for changing the status, if required, and click **Yes**.
   The certificate status is changed as per the selection.

Assigning Certificate Group for Server Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a server certificate to a group:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the certificate that you want to assign to a group to.
3. From the **Actions** dropdown, click **Assign Group**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **Assign to Group** pop-up window that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Unassigning Certificate Group from Server Certificates

You can unassign any certificates from a specific certificate group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, select the certificate that you want to unassign from a certificate group.
3. From the **Actions** dropdown, click **Unassign Group**.
4. In the **Unassign Group** window that is displayed, enter the reason for unassigning the certificate from the group and click **Unassign**.
   The selected certificate is now assigned to the default group.

Bulk Revoking Server Certificates

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

To bulk revoke server certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the checkbox for the required certificate.
3. Click **Actions**, and then select **Revoke Certificate** from the list.
   The certificate revoke dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The following table describes the options available on the revoke certificate page:

Field descriptions for certificate revoke

Field	Description
***Reason**	The required option from the dropdown list. The possible options are, • **Key Compromise** • **Affiliation Changed** • **Superseded** • **Cessation of Operation**.
Comments	Enter any additional comments, if required.
**: Mandatory fields*	

4. Click **Yes**.

Updating Certificate Attributes for Server Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attribute for a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, select the certificate for which you want to update attributes.
3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

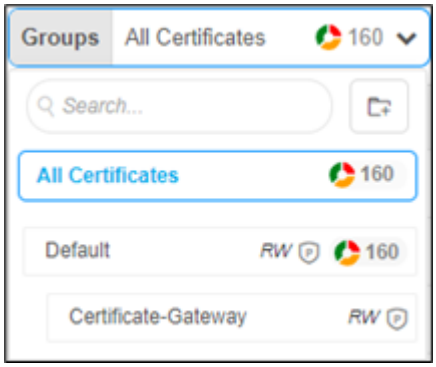
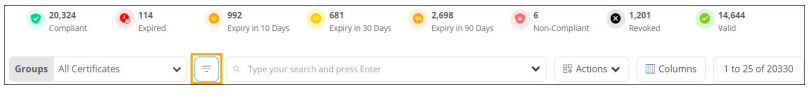
From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

Managing the Client Certificate Inventory

Client certificate inventory displays all the client certificates with the EKU (Extended/enhanced key usage) client authentication, email protection. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform action such as bulk certificates renewal/revocation check/CA migration, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

On the **Certificate Inventory** > **Client** certificate page, all the client certificates are listed. You can perform the following actions:

Options available on the Client Certificate inventory page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates. 
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options available on the Client Certificate inventory page (continued)

Options	Description
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates.
Columns	Allows you to select the columns to be displayed on the Client Certificate inventory page **Note:** In the current implementation, the **Certificate Type** column is populated for only selected CAs. To populate it for the SwissSign CA, see the instructions here.
Toggle	Allows you to toggle between the following display options for the Client Certificate inventory: • **Reports**: Displays reports related to client certificates. For more information, click here. • **List**: Displays the list of client certificates.

The list of actions you can perform on the certificates are:

- Export Certificates - To export the server certificate.
- Download Certificates - To download a certificate from an inventory to a file (the private key, root, and intermediate certificates can be included in the download.
- Delete - To delete the server certificate.
- Change Status - To change the server certificate status.
- Assign Group - To assign a group to the certificate.
- Unassign Group - To unassign a group from the certificate.
- Add/Modify Comments - To add/modify comments to the certificate.
- Certificate Attributes - To update the certificate attributes.
- Bulk Update Attributes Value - To update the certificate attributes for certificates.
- Renew Certificates - To renew certificates before expiry.
- Revoke Certificates - To revoke certificates
- CA Switch - Switching to another Certificate Authority (CA) for your SSL needs.
- Revocation Check - To check the revocation status of the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Populating the Certificate Type Column for the SwissSign CA

In the current implementation, for the SwissSign CA, the certificate type column is not auto populated on display. To populate it:

1. Run the Certificate Authority discovery scan for SwissSign CA.
2. For the discovered certificates, manually modify the status to **Managed** or **Monitored**.

   The certificate type for each SwissSign certificate is added to the column.

   The data is additionally leveraged to generate reports for SwissSign CA, categorized by certificate type.

What's Next

Once you have discovered certificates, you are ready to proceed with any of the following certificate actions:

- If you want to Auto Renew the Discovered Certificate.
- If you want to Auto Regenerate the Discovered Certificate.
- Exporting a Client Certificate
- Adding/Modifying Comments for Client Certificates
- Editing Client Certificate Details via the Connector
- Deleting Client Certificates
- Changing Client Certificate Status
- Assigning Certificate Group to Client Certificates
- Unassigning Certificate Group from Client Certificates
- Bulk Revoking Client Certificates
- Updating Certificate Attributes for Client Certificates
- Bulk Updating Certificate Attributes

Exporting a Client Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in **.xls** or **.csv** format. This can be used for reporting or creating an inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To export a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Server Certificate** page is displayed.
2. On the **Client Certificate** page, select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** dialog box is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Adding/Modifying Comments for Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate that you want to revoke.
3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** pop-up window that is displayed, enter a comment and click **Save**.

Editing Client Certificate Details via the Connector

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. Open the holistic view of the certificate you want to edit.
3. In the holistic view, hover over the connector you want to edit.
4. From the menu displayed, click **Edit**.
   The **Client certificate > <certificate name>** page is displayed.
5. Edit the certificate details as required.
   For field descriptions and instructions see Enrolling a Client Certificate.

Deleting Client Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any reports and alerts.

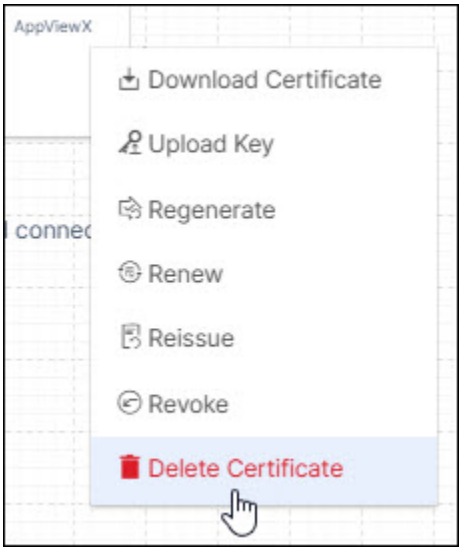
Deleting Individual Client Certificates from the Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. From the **Client Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

Deleting Client Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. From the **Client Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) icon and from the menu displayed, click **Delete Certificate**.

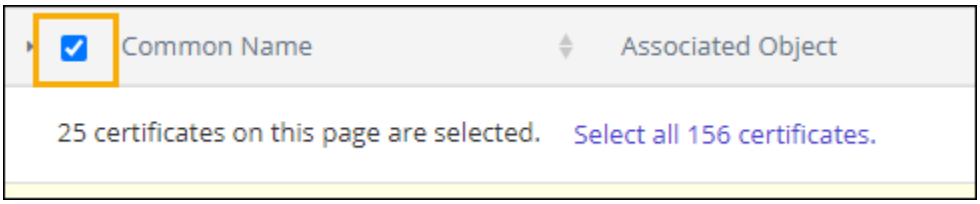


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

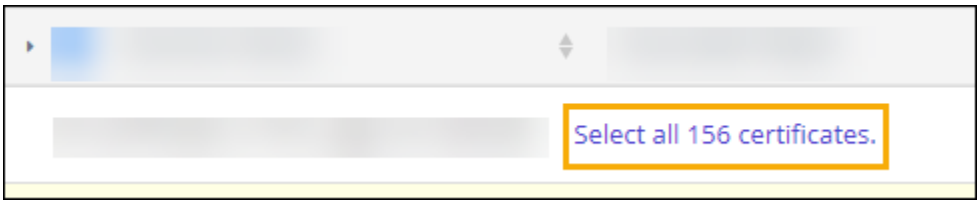
4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The client certificate is deleted from the AppViewX inventory.

Deleting all Client Certificates

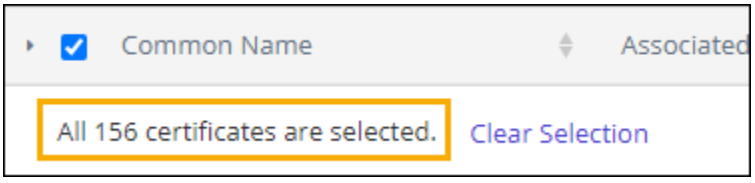
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. In the **Client Certificate** inventory, select the checkbox next to the **Common Name** field.



   All certificates on the current page are selected.
3. To select all certificates in the client certificate inventory, click **Select all <no. of certificates> certificates**.



   This will select all certificates across all pages in the client certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certificate** confirmation dialog box, click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

All certificates in the client certificate inventory are deleted.

Note: The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.

Example: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificates will be deselected.

Changing Client Certificate Status

The status of a certificate can be set as monitored or managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, you can only view the certificate details in reports and in the inventory. When the certificates are set as Managed, the certificate-related actions along with push/bind operations can be performed along with viewing of the certificates in the reports and inventory.

To change the client certificate status:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate for which you want to change status.
3. From the **Actions** dropdown, click **Change Status**.
4. In the **Change Status** pop-up window that is displayed, in the **Change Status to** field, select the status of the certificate field as **Managed** or **Monitored**.
5. Enter the reason for changing the status, if required, and click **Yes**.
   The certificate status is changed as per the selection.

Assigning Certificate Group to Client Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a client certificate to a group:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate that you want to assign to a group.
3. From the **Actions** dropdown, click **Assign Group**.
4. In the **Assign to Group** pop-up window that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.

   The certificate is assigned to the selected group.

Unassigning Certificate Group from Client Certificates

The user can unassign any certificates from the specific group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.

   The **Client Certificate** page is displayed.
2. In the **Common Name** column certificate list, select the desired certificate(s) that you want to unassign the certificate group.
3. Click the **List** toggle button on the right top corner of the client certificate page.
4. Click **Actions**, and then select **Unassign Group** from the drop-down list.
5. The selected certificate is assigned to the default group.

   The following message is displayed: **<certificate_name> assign to undefined**.

Bulk Revoking Client Certificates

Note: For the DevOps users, the issuing CA may disable the revoke action. In this case, a pop-up message, informing the user of this, is displayed. For enterprise users, the revoke action is enabled.

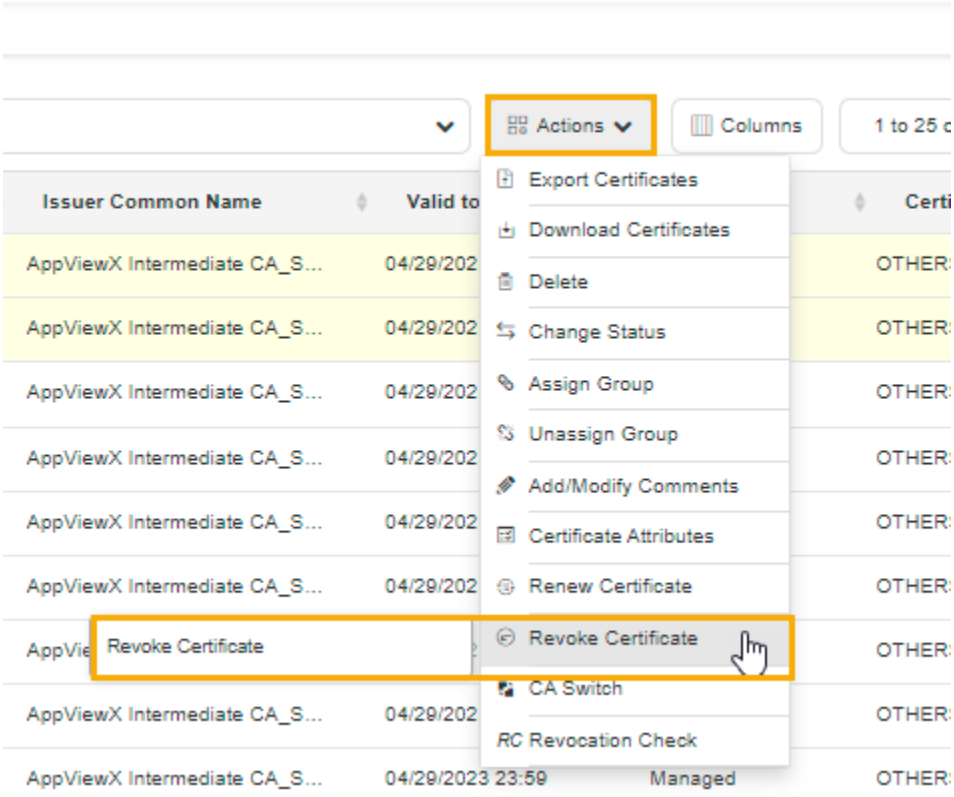
To bulk revoke a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.

   The **Client Certificate** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click the **List** toggle button on the right top corner of the server certificate page.



3. Select the required certificate check box.
4. Click **Actions**, and then select **Revoke Certificate** from the list.

   The certificate revoke dialog box is displayed.

   The following table describes the options available on the revoke certificate page:

Field description for certificate revoke

Field	Description
***Reason**	The required option from the dropdown list. The possible options are: • **Key Compromise** • **Affiliation Changed** • **Superseded** • **Cessation of Operation**.
Comments	Enter additional details, if required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

5. Click **Yes**.

Updating Certificate Attributes for Client Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attribute for a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
2. On the **Client Certificate** page, select the certificate for which you want to update attributes.
3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).

5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

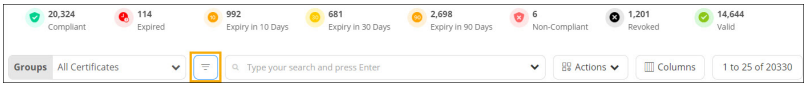
Managing the Code Signing Certificate Inventory

Code signing certificate inventory displays all the code certificate with the EKU (Extended/enhanced key usage) code signing will be present. The certificates in this inventory will be shown to the user only based on role-based access control on the certificate group. From this inventory, the user can select one or many certificates and perform bulk certificates revocation check, search and filter certificates, export certificates, download certificates, delete certificates, and so on.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

On the **Certificate Inventory** > **Code Signing** certificate page, all the code signing certificates are listed. You can perform the following actions:

Options available on the Code Signing Certificate page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates.
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 
Search bar	Allows you to search for a certificate(s) within the server certificate inventory using keywords.
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates.
Columns	Allows you to select the columns to be displayed on the Code Signing Certificate inventory page.
Toggle	Allows you to toggle between the following display options for the Code Signing Certificate inventory: • **Reports**: Displays reports related to Code Signing certificates. For more information, click here. • **List**: Displays the list of server certificates.

The list of actions you can perform on the certificates are:

- Export Certificates - To export the server certificate.
- Download Certificates - To download a certificate from an inventory to a file (the private key, root, and intermediate certificates can be included in the download.
- Delete - To delete the server certificate.
- Change Status - To change the server certificate status.
- Assign Group - To assign a group to the certificate.
- Unassign Group - To unassign a group from the certificate.
- Add/Modify Comments - To add/modify comments to the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Certificate Attributes - To update the certificate attributes.
- Bulk Update Attributes Value - To update the certificate attributes for certificates.
- Revocation Check - To check the revocation status of the certificate.

What's Next

Once you have discovered certificates, you are ready to proceed with any of the following certificate actions:

- If you want to Auto Renew the Discovered Certificate.
- If you want to Auto Regenerate the Discovered Certificate.
- Exporting a Code Signing Certificate
- Adding/Modifying Comments for Code Signing Certificates
- Editing Code Signing Certificate Details via the Connector
- Deleting Code Signing Certificates
- Changing Code Signing Certificate Status
- Assigning Certificate Group for Code Signing Certificates
- Unassigning Certificate Group from Code Signing Certificates
- Updating Certificate Attributes for Code Signing Certificates
- Bulk Updating Certificate Attributes

Exporting a Code Signing Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in **.xls** or **.csv** format. This can be used for reporting or creating an inventory.

To export a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** dialog box is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Adding/Modifying Comments for Code Signing Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to revoke.
3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** pop-up window that is displayed, enter a comment and click **Save**.

Editing Code Signing Certificate Details via the Connector

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. Open the holistic view of the certificate you want to edit.
3. In the holistic view, hover over the connector you want to edit.
4. From the menu displayed, click **Edit**.
   The **Code signing certificate > <certificate name>** page is displayed.
5. Edit the certificate details as required.
   For field descriptions and instructions see Enrolling a Code Signing Certificate.

Deleting Code Signing Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any of the reports and alerts.

Deleting Individual Code Signing Certificates from the Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. From the **Code Signing Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

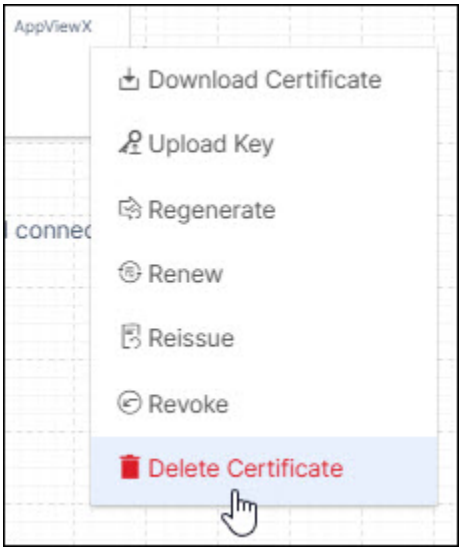
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Deleting Code Signing Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. From the **Code Signing Certificate** inventory, click the **Common Name** of the certificate you want to delete.

   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) button and from the menu displayed, click **Delete Certificate**.

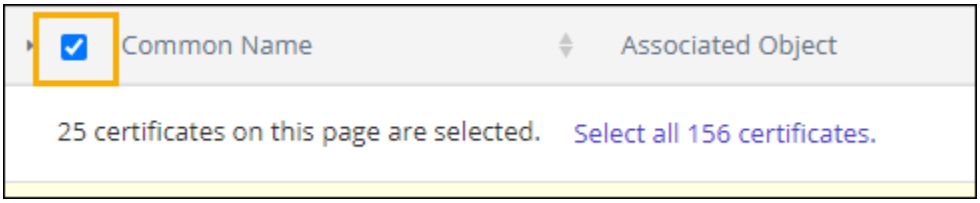


4. In the **Confirmation** dialog box that is displayed, click **Yes**.

   The code signing certificate is deleted from the AppViewX inventory.

Deleting all Code Signing Certificates

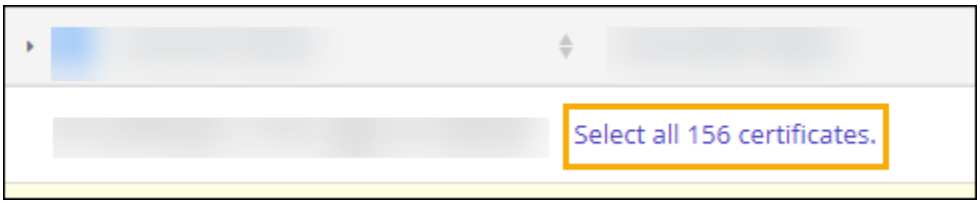
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. In the **Code Signing Certificate** inventory, select the checkbox next to the **Common Name** field.



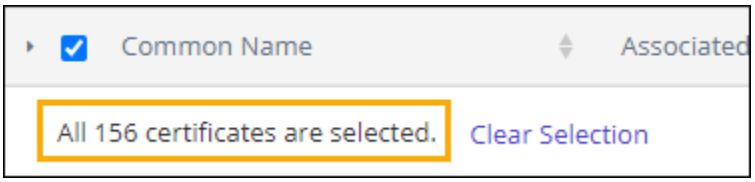
   All certificates on the current page are selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. To select all certificates in the code signing certificate inventory, click **Select all <no. of certificates> certificates**.



This will select all certificates across all pages in the code signing certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   All certificates in the code signing certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificates will be deselected.

Changing Code Signing Certificate Status

The status of a certificate can be set as monitored or managed during or after the certificate discovery process and also from the certificate inventory directly. When the certificates are set as Monitored, you can only view the certificate details in reports and in the inventory. When the certificates are set as Managed, the certificate-related actions along with push/bind operations can be performed along with viewing of the certificates in the reports and inventory.

To change the code signing certificate status:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate for which you want to change status.
3. From the **Actions** dropdown, click **Change Status**.
4. In the **Change Status** dialog box that is displayed, in the **Change Status to** field, select the status of the certificate field as **Managed** or **Monitored**.
5. Enter the reason for changing the status, if required, and click **Yes**.
   The certificate status is changed as per the selection.

Assigning Certificate Group for Code Signing Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a certificate group to a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to assign to a group.
3. From the **Actions** dropdown, click **Assign Group**.
4. In the **Assign to Group** dialog box that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.
6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Unassigning Certificate Group from Code Signing Certificates

You can unassign any certificates from a specific certificate group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate that you want to unassign from a certificate group.
3. From the **Actions** dropdown, click **Unassign Group**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **Unassign Group** window that is displayed, enter the reason for unassigning the certificate from the group and click **Unassign**.
   The selected certificate is now assigned to the default group.

Updating Certificate Attributes for Code Signing Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attributes for a code signing certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
2. On the **Code Signing Certificate** page, select the certificate for which you want to update attributes.
3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

   Note: Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

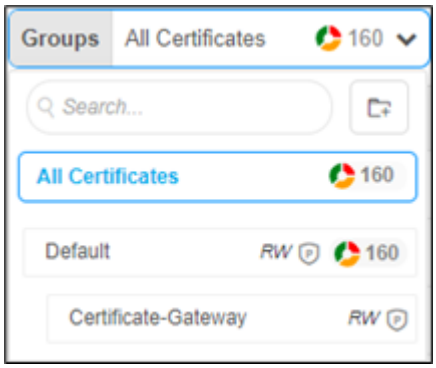
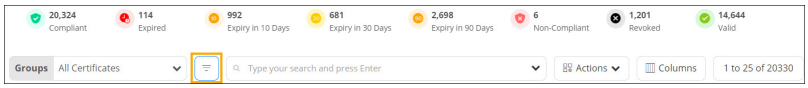
Managing the Device Certificate Inventory

Device certificate inventory displays all the management interface certificates. Currently, in this inventory, only F5 vendor certificates are shown.

On the **Certificate Inventory** > **Device** page, all the device certificates are listed. You can perform the following actions:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options available on the Device Certificate inventory page

Options	Description
Groups	Expanding this dropdown displays the certificate groups and the number of certificates in each group. Selecting a group will display the filtered list of certificates. 
Filter Summary	Displays the status of certificates according to expiry, compliance, validity, and so on. 
Advanced Search	Allows you to perform a quick search for specific data. Clicking on the search bar dropdown opens the **Advanced Search** window.
Actions	Displays the list of actions you can perform on the certificates.
Columns	Allows you to select the columns to be displayed on the Device Certificate inventory page.
Toggle	Allows you to toggle between the following display options for the Server Certificate inventory: • **Reports**: Displays reports related to server certificates. • **List**: Displays the list of server certificates.

The list of actions you can perform on the certificates are:

- Export Certificates - To export the server certificate.
- Delete - To delete the server certificate.
- Assign Group - To assign a group to the certificate.
- Unassign Group - To unassign a group from the certificate.
- Add/Modify Comments - To add/modify comments to the certificate.
- Certificate Attributes - To update the certificate attributes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Bulk Update Attributes Value - To update the certificate attributes for certificates.
- Renew Certificates - To renew certificates before expiry.
- Revocation Check - To check the revocation status of the certificate.

- Exporting a Device Certificate
- Deleting Device Certificates
- Assigning Certificate Group to Device Certificates
- Unassigning Certificate Group from Device Certificate Groups
- Adding/Modifying Comments for Device Certificates
- Updating Certificate Attributes for Device Certificates
- Bulk Updating Certificate Attributes
- Downloading Failed Updates

Exporting a Device Certificate

Export certificate action allows the user to export certificate details in the form of columns and values. The user can export all the certificates in the inventory or select only specific certificates and export. The output of this action can be selected in **.xls** or **.csv** format. This can be used for reporting or creating an inventory.

To export a device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to export.
3. From the **Actions** dropdown menu, select **Export Certificates**.
   The **Export** dialog box is displayed.
4. Select the required **Options** and **Format**.
   The selected certificate is exported to your local machine.

Deleting Device Certificates

AppViewX lets you delete individual certificates, selected certificates, and all certificates from the server certificate inventory.

Note: Once a certificate is deleted from the inventory, it will not be displayed in any reports and alerts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Deleting Individual Device Certificates from the Inventory

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. From the **Device Certificate** inventory, for the certificate(s) you want to delete, select the corresponding checkboxes.
3. From the **Actions** dropdown menu, select **Delete**.
4. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   The selected certificate(s) will be deleted.

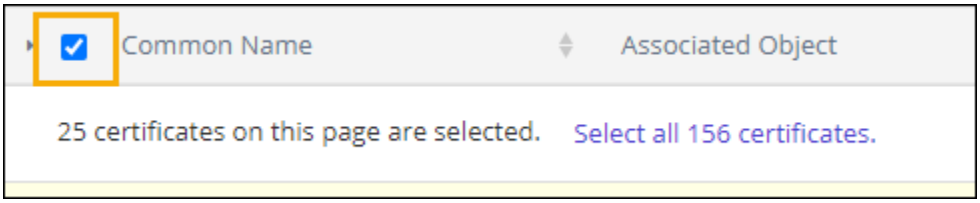
Deleting Device Certificates from the Holistic View

Note: Via the holistic view, you can delete only one certificate at a time.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. From the **Device Certificate** inventory, click the **Common Name** of the certificate you want to delete.
   The holistic view of the selected certificate is displayed.
3. Hover your mouse over the (**More**) icon and from the menu displayed, click **Delete Certificate**.
4. In the **Confirmation** dialog box that is displayed, click **Yes**.
   The device certificate is deleted from the AppViewX inventory.

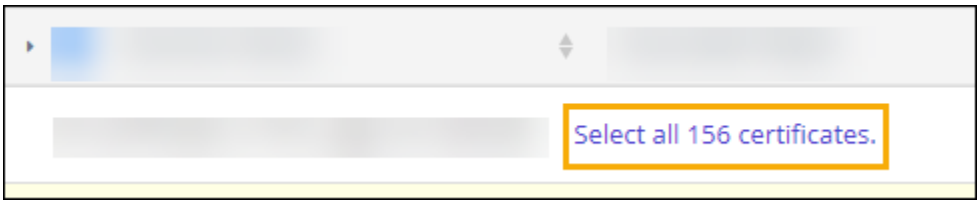
Deleting All Device certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. From the **Device Certificate** inventory, select the checkbox next to the **Common Name** field.

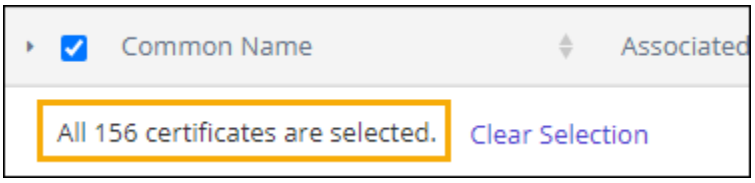


   All certificates on the current page are selected.
3. To select all certificates in the device certificate inventory, click **Select all <no. of certificates> certificates**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



This will select all certificates across all pages in the device certificate inventory.



4. From the **Actions** dropdown menu, select **Delete**.
5. From the **Delete Certificate** confirmation dialog box, click **Yes**.
   All certificates in the device certificate inventory are deleted.

> **Note:** The **Select all <no. of certificates> certificates** option does not allow deselecting individual certificates. If, after selecting all the certificates, you deselect a few certificates, only the remaining certificates on the current page will remain selected. The certificates on the other pages of the inventory will be deselected automatically.
>
> **Example**: Assume you have 150 certificates in your inventory and each page is set to display 25 records. If you select all 150 certificates and then deselect two certificates from the first page, only the remaining 23 certificates on the first page will be selected. The other 125 certificates will be deselected.

Assigning Certificate Group to Device Certificates

The certificates with common attributes can be grouped together to perform compliance checks against policy details, to enable auto-renewal and auto-push operations. You can also view certificates as groups.

To assign a certificate group to device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to assign to a group.
3. From the **Actions** dropdown, click **Assign Group**.
4. In the **Assign to Group** pop-up window that is displayed, search for the group that you want this certificate to be assigned to.
5. Select the required certificate group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Enter a reason for assigning the certificate to the selected certificate group, if required, and click **Assign**.
   The certificate is assigned to the selected group.

Unassigning Certificate Group from Device Certificate Groups

You can unassign any certificates from a specific certificate group to the default group. The policy and actions of the default group will be applied to these certificates.

To unassign a certificate group assigned to a device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to unassign from a certificate group.
3. From the **Actions** dropdown, click **Unassign Group**.
4. In the **Unassign Group** window that is displayed, enter the reason for unassigning the certificate from the group and click **Unassign**.
   The selected certificate is now assigned to the default group.

Adding/Modifying Comments for Device Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate that you want to revoke.
3. From the **Actions** dropdown, click **Add/Modify Comments**.
4. In the **Add/Modify Comments** dialog box that is displayed, enter a comment and click **Save**.

Updating Certificate Attributes for Device Certificates

Other than the fields that are defined for CSR, you can add organization-specific values to a request. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes.

To update the certificate attributes for a device certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
2. On the **Device Certificate** page, select the certificate for which you want to update attributes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. From the **Actions** dropdown, click **Certificate Attributes**.
4. Update the **Certificate Attributes** and click **Save**.

Bulk Updating Certificate Attributes

Bulk Updating Attributes using a CSV File

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

> **Note:** Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **File Upload**.
4. Click **Download Template**.
   A **.csv** file will be downloaded to your system. This file has the format in which you need to specify the attributes and their corresponding updated values (along with the certificate identification details).
5. In the **Upload File** field, click **Upload**.
6. Navigate to the location where the updated **.csv** file is saved on your system and upload the file.
7. Click **Save**.

Bulk Updating Attributes for a Certificate Group

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. From the **Actions** menu, select **Bulk Update Attributes Value**.
   The **Bulk Update Attributes Value** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. Ensure that no updates are made to attributes involved in an expiry alert. (To check this, go to (**Menu**) > **CERT+** > **Administration** > **Certificate Attributes**.)

3. From the options for **Update Method**, select **Based on Certificate Group**.
4. From the dropdown list, select the required **Certificate Group**.
5. From the dropdown list, select one or more **Cert Attributes** that you want to update.
   Corresponding text/list fields are displayed depending on the **Cert Attributes** selected.
6. Enter the required value for each attribute selected in the corresponding field.
7. Click **Save**.

Downloading Failed Updates

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

Downloading Failed Updates

From the **Bulk Update Attributes Value** dialog box, to view failed bulk updates to the certificate attributes, click **Download Failed Updates**.
A **.csv** file with a log of the failed updates is downloaded to your local system.

Managing the Intermediate Certificate Inventory

Intermediate certificate inventory is where the issuer certificates apart from the root certificate will be displayed. In the chain of trust, if there is more than one layer of the intermediate certificate (excluding root and end certificate), all those certificates will be shown in this inventory. From this inventory, the user can get into the holistic view where the user can perform the push operation of the intermediate and its root certificates.

Options available on the Intermediate Certificate page

Options	Description
Search bar	Allows you to search for a certificate(s) within the server certificate inventory using keywords and by Certificate Authority.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options available on the Intermediate Certificate page (continued)

Options	Description
Actions	Displays the list of actions you can perform on the certificates. **Note:** This dropdown is enabled only when you select at least one certificate from the inventory.
Columns	Allows you to select the columns to be displayed on the **Intermediate Certificate** page.

• Deleting an Intermediate Certificate

Deleting an Intermediate Certificate

You can delete a certificate from the intermediate certificate inventory in AppViewX. Once the certificate gets deleted from the inventory, the same will not be displayed in reports and alerts.

To delete an intermediate certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Intermediate**.
2. On the **Intermediate Certificate** page, select the certificate that you want to delete.
3. From the **Actions** dropdown menu, select **Delete**.
4. In the **Delete Certificate** dialog box that is displayed, click **Yes**.
   The intermediate certificate is deleted from AppViewX inventory.

Managing the Root Certificate Inventory

Root certificate inventory displays the root certificates for all the issuers. For any chain of trust certificates, there can be only one root certificate. From this inventory, you can get into the holistic view and perform the push operation for the root certificate only.

Options available on the Root Certificate page

Options	Description
Search bar	Allows you to search for a certificate(s) within the server certificate inventory using keywords and by Certificate Authority.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Options available on the Root Certificate page (continued)

Options	Description
Actions	Displays the list of actions you can perform on the certificates. **Note:** This dropdown is enabled only when you select at least one certificate from the inventory.
Columns	Allows you to select the columns to be displayed on the **Intermediate Certificate** page.

• Deleting a Root Certificate

Deleting a Root Certificate

You can delete a certificate from the root certificate inventory in AppViewX. Once the certificate gets deleted from the inventory, the same will not be displayed in reports and alerts.

To delete a root certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Root**.
2. On the **Root Certificate** page, select the certificate that you want to delete.
3. From the **Actions** dropdown menu, select **Delete**.
4. In the **Delete Certificate** dialog box that is displayed, click **Yes**.
   The root certificate is deleted from AppViewX inventory.

Uploading a Certificate

You can upload either the end certificate or trust store certificates in the certificate inventory. Once uploaded, the certificate will be applied by the policy based on the associated certificate group.

To upload a certificate,

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Upload**.
   The **Upload Certificate** page is displayed.
2. Enter/Select the **Upload Certificate**details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions on for uploading a certificate

Field	Description
Certificate Type	Click the check box to select the desired certificate type. The possible types are: • End Certificate • CA Certificate.
Certificate Group	Select the desired group from the dropdown list.
***Certificate**	Click **Browse** to upload the certificate-key files from your computer.
Comments	Enter a description in this field. **Note:** Character limit: **2000 characters**

3. Click **Upload**.

Note: Ensure that the uploaded **Certificate-Keys** file is stored in the Certificate Group.

Downloading Certificates

- Downloading Server Certificates
- Downloading Client Certificates from the Holistic View
- Downloading Device Certificates from the Holistic View
- Downloading Code Signing Certificates from the Inventory
- Downloading Intermediate Certificates
- Downloading Root Certificates

Downloading Server Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Downloading Server Certificates from the Inventory

Server certificates can be downloaded from the server inventory as well as in the holistic view. In the server inventory, the user can select one or more certificates and download them in <.*crt*> format with/ without private keys and also with/without their respective trust store certificates.

To download server certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. In the **Common Name** column certificate list, select the desired certificate(s) that you want to download.
3. Click **Actions**, and then select **Download Certificates** from the list.
   The **Download Certificates** dialog box is displayed.
   a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.
   b. You can also enable/disable **the Download Truststore Certificates** option along with the end certificates.

   > **Note:** If you have permission to view the restricted content mentioned in Step 7, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

   c. The system enables the **Secret Passphrase** field when you select **Certificates and Keys**. Enter a passphrase to encrypt the contents into a <.zip> file.
4. Click **Download**.
   The certificate is downloaded to your local machine.
5. To view details of the certificate, unzip the file and open the security certificate file.
6. Click **Details**.

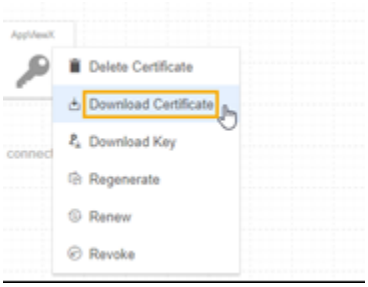
Downloading Server Certificates from the Holistic View

Server certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download server certificates via the holistic view:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. On the **Server Certificate** page, click the **Common Name** of the certificate you want to download.
   The holistic view of the certificate is displayed.
3. Hover your mouse over and select **Download Certificate** from the options displayed.



   The **Download Certificate** pop-up window is displayed.
4. In the **Download Certificate** pop-up window that is displayed, select the file format from the **Certificate type** dropdown and click **Yes**.

> **Note:** For PEM and DER certificate types, you can turn the **Download Truststore Certificates** toggle On/Off.

   The certificate(s) is downloaded to your local machine.

Downloading Client Certificates from the Holistic View

Client certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download client certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Client**.
   The **Client Certificate** page is displayed.
2. On the **Client Certificate** page, click on the **Common Name** of the certificate that you want to download.
   The holistic view of the certificate is displayed.
3. Hover your mouse over and select **Download Certificate** from the options displayed.
   The **Download Certificate** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Select the file format from the **Certificate Type** list.
b. For PEM and DER certificate types, you can use the toggle button to On/Off in the **Download Truststore Certificates** option along with end certificates.

4. In the **Download Certificate** pop-up window that is displayed, select the file format from the **Certificate type** dropdown and click **Yes**.

> **Note:** For PEM and DER certificate types, you can turn the **Download Truststore Certificates** toggle On/Off.

The certificate(s) is downloaded to your local machine.

Downloading Device Certificates from the Holistic View

Device certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download device certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Device**.
   The **Device Certificate** page is displayed.
2. On the **Device Certificate** page, click the **Common Name** of the certificate you want to download.
   The holistic view of the certificate is displayed.
3. Hover your mouse over and select **Download Certificate** from the options displayed.
   The **Download Certificate** dialog box is displayed.
4. In the **Download Certificate** pop-up window that is displayed, select the file format from the **Certificate type** dropdown and click **Yes**.

> **Note:** For PEM and DER certificate types, you can turn the **Download Truststore Certificates** toggle On/Off.

The certificate(s) is downloaded to your local machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Downloading Code Signing Certificates from the Inventory

Code Signing certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download code signing certificates via the holistic view:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Code Signing Certificate**.
   The **Code Signing Certificate** page is displayed.
2. On the **Code Signing Certificate** page, select the certificate(s) that you want to download.
3. From the **Actions**dropdown, click **Download Certificates**.
   The **Download Certificates** pop-up window is displayed.
   a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.
   b. You can also enable/disable **Download Truststore Certificates** option along with the end certificates.

   > **Note:** If you have permission to view the restricted content, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

   c. The system enables the **Secret Passphrase** field when you select the **Certificates and Keys** option. Enter a passphrase to encrypt the contents into a *<.ZIP>* file.
4. In the **Download Certificate** dialog box, enter or select the requested filed information.

Field Description for Download Certificate

Field	Description
Choose Download Type	Select the certificate download type as: • **Certificate Only** • **Certificate and Keys**
Download Truststore Certificates	Turn on this toggle to download truststore certificates.
Set Password for Keystore	Enter a passphrase to encrypt the contents into a **.zip** file.

   a. In the **Download Certificate** pop-up window, select **Certificates Only** or **Certificates and Keys**.
   b. You can also enable/disable **the Download Truststore Certificates** option along with the end certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** If you have permission to view the restricted content mentioned in Step 7, the certificate details are downloaded with <.zip> file. If you do not have the necessary permissions, the system creates and downloads an empty <.zip> file to the destination you specify.

c. The system enables the **Secret Passphrase** field when you select **Certificates and Keys**. Enter a passphrase to encrypt the contents into a <.zip> file.

5. Click **Download**.
6. To view details of the certificate, unzip the file and open the security certificate file.
7. Click **Details**.

Downloading Intermediate Certificates

Downloading Intermediate Certificates from the Inventory

You can download intermediate certificate(s) in PEM format with or without its trust store certificates.

To download intermediate certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Intermediate**.
   The **Intermediate Certificate** page is displayed.
2. On the **Intermediate Certificate** page, select the certificate(s) that you want to download.
3. From the **Actions**dropdown, click **Download**.
   The certificate is downloaded to your local machine.
4. To view details of the certificate, unzip the file and open the security certificate file.
5. Click **Details**.

Downloading an Intermediate Certificate from the Holistic View

Intermediate certificates can be downloaded via holistic view only one certificate at a time in multiple formats as PEM, DER, PKCS#7, PKCS#12, and JKS. PKCS#12 and JKS can be downloaded only with the password-protected certificate.

To download an intermediate certificate via the holistic view:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Intermediate**.
2. On the **Intermediate Certificate** page, click the **Common Name** of the certificate that you want to download from the holistic view.
   The holistic view of the certificate is displayed.
3. Hover your mouse over the (**More**) button and click **Download Certificate**.
4. In the **Download Certificate** pop-up window that is displayed, select the **Certificate type** from the options available in the dropdown.
5. For PEM and DER certificate types, turn on the **Download Truststore Certificates** toggle.
6. Click **Yes**.
   The certificate is downloaded to your local machine.

Downloading Root Certificates

Downloading Root Certificates from the Inventory

Download root certificate is the action to download root certificate, the certificate get downloaded in PEM **.*crt** format from the inventory.

To download root certificates from the inventory:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Root**.
   The **Root Certificate** page is displayed.
2. On the **Root Certificate** page, select the certificate(s) that you want to download.
3. From the **Actions**dropdown, click **Download**.
   The certificate is downloaded to your local machine
4. To view details of the certificate, unzip the file and open the security certificate file.
5. Click **Details**.

Downloading a Root Certificate from the Holistic View

Download root certificate is the action to download root certificate in PEM format with or without its trust store certificates.

To download a root certificate via the holistic view,

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Root**.
   The **Root Certificate** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. In the **Common Name** column certificate list, select the desired certificate that you want to download the CA.
   The holistic view is displayed.
3. Click the (**More**) icon in the holistic view, and then select **Download Certificate** from the list.
   The **Download Certificate**dialog box is displayed.
4. Select the file format from the **Certificate type** list.
5. Click **Yes**.
   The certificate is downloaded to your local machine.

Archiving Certificates

Certificate archival is a best practice that helps with post-lifecycle certificate management. Certificate archives are a historical record that are useful for legal, operational, and strategic requirements.

The feature enables automatic archival of certificates that have been renewed, revoked, regenerated, or expired, ensuring that older certificate versions are retained for reference and audit purposes without cluttering the active inventory. Archival actions can be triggered through manual UI operations, automation workflows, or API requests, with audit logs capturing the user and source details.

Archived certificates appear in the discovery inventory with **Status** = **Archived**. Unlike active certificates, they are not moved to the certificate category inventories but are instead stored in the Archived Certificates inventory.

Certificates in the archived inventory are excluded from discovery scans, issuance workflows, alerts, and active certificate counts, ensuring cleaner operational management while preserving a complete lifecycle history.

ACF Permissions Required for Certificate Archival and Recovery

For Archiving Certificates

1. Go to (**Menu**) > **Platform** > **Identity** . **Role**.
   The **Role** inventory is displayed.
2. To enable certificate archival for a role, click the corresponding role **Name**.
   The **Role > Modify :: <role name>** page is displayed.
3. Go to the **Authorized Functions** tab.
4. For the selected role:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- To enable certifcate archival for server certificates, go to **Cert+** > **Certificate Inventory** > **Server** and select the checkbox for **Archive Certificates**.
- To enable certifcate archival for client certificates, go to **Cert+** > **Certificate Inventory** > **Client** and select the checkbox for **Archive Certificates**.
- To enable certifcate archival for code signing certificates, go to **Cert+** > **Certificate Inventory** > **Code signing** and select the checkbox for **Archive Certificates**.

For Recovering Certificates

1. Go to (**Menu**) > **Platform** > **Identity** . **Role**.
   The **Role** inventory is displayed.
2. To enable certificate recovery for a role, click the corresponding role **Name**.
   The **Role > Modify :: <role name>** page is displayed.
3. Go to the **Authorized Functions** tab.
4. For the selected role, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **Restore**.
5. Click **Save**.

For Viewing the Archived Certificates Inventory

1. Go to (**Menu**) > **Platform** > **Identity** . **Role**.
   The **Role** inventory is displayed.
2. To enable viewing the certificate inventory for a role, click the corresponding role **Name**.
   The **Role > Modify :: <role name>** page is displayed.
3. Go to the **Authorized Functions** tab.
4. For the selected role, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **View inventory**.
5. Click **Save**.

For Managing Certificates in the Archived Certificates Inventory

1. Go to (**Menu**) > **Platform** > **Identity** . **Role**.
   The **Role** inventory is displayed.
2. To enable viewing the certificate inventory for a role, click the corresponding role **Name**.
   The **Role > Modify :: <role name>** page is displayed.
3. Go to the **Authorized Functions** tab.
4. For the selected role:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- To enable inventory view customization, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **Columns**.

  This will give the role the permission to show and hide columns in the Archived Certificates inventory, as required.

- To enable exporting certificates from the Archived Certificates inventory, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **Export**.
- To enable deletion of certificates from the Archived Certificates inventory, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **Delete**.

5. For the selected role, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **View inventory**.
6. Click **Save**.

For Configuring Auto Archival and Recovery Settings

1. Go to (**Menu**) > **Platform** > **Identity** . **Role**.
   The **Role** inventory is displayed.
2. To enable viewing the certificate inventory for a role, click the corresponding role **Name**.
   The **Role > Modify :: <role name>** page is displayed.
3. Go to the **Authorized Functions** tab.
4. For the selected role, go to **Cert+** > **Certificate Inventory** > **Archive** and select the checkbox for **Settings**.
5. Click **Save**.

Archiving Certificates

Ensure that you have the required ACF permissions for archiving certificates.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the certificate type for viewing the inventory.
   For example, to view the certificate inventory for server certificates, under **CERTIFICATE INVENTORY**, select **Server**.
   The inventory page for the selected certificate type is displayed.
2. From the certificate inventory, select the checkbox for certificate you want to archive.
   You can also select multiple certificates.
3. From the **Actions** dropdown menu, select **Archive**.
   A confirmation dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. (Optional) From the **Reason** dropdown list, from the following options, select a reason for archiving the certificate:
   - **Renewed**
   - **Regenerated**
   - **Revoked**
   - **Expired**
   - **Deprecated**
   - **Others**

   The archived certificate is moved to the Archived Certificates inventory.

Viewing the Archived Certificates Inventory

Ensure that you have the required ACF permissions for viewing the Archived Certificates inventory.

Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Archived Certificates**.
The **Archived Certificates** inventory is displayed.

The **Archived Certificates** inventory structure is explained here.

Understanding the Archived Certificates Inventory

The table below explains the structure of the **Archived Certificates** inventory.

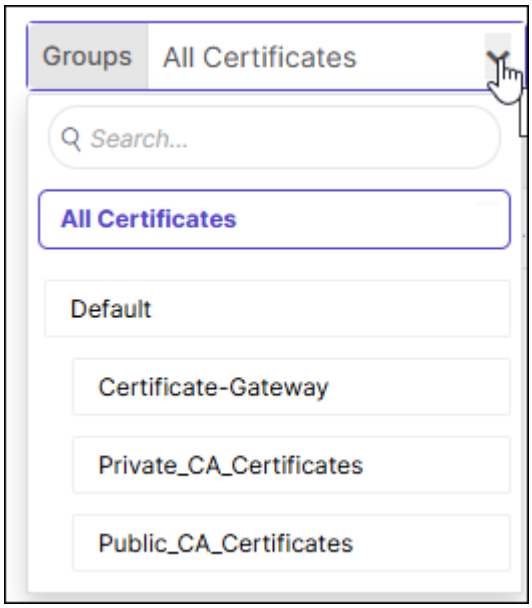
The inventory provides a comprehensive set of columns to display certificate metadata and supports pagination, search, and filter functionalities, making it easy to locate specific certificates and understand their archival context.

Archived Certificates Inventory Structure

Column/Field	Description
Groups	Use the **Groups** dropdown menu to filter the inventory and display only certificates associated with the selected groups.

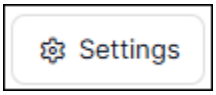
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Archived Certificates Inventory Structure (continued)

Column/Field	Description
	
Search	Use the search field to execute a free text certificate search on certificate metadata such as common name, Subject Alternative Names, serial number, issuer, and so on.
	Use the **Actions** dropdown menu to: • **Recover** archived certificates. Ensure that you have the required ACF permissions to recover archived certificates. For instructions and post-recovery status details, see Recovering Archived Certificates. • **Export** archived certificates' data (in the CSV and XLSX formats, for all/selected columns). Ensure that you have the required ACF permissions to export certificates from the archived inventory. For indicative instructions, see Exporting Server Certificates. • **Delete** archived certificates from this inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Archived Certificates Inventory Structure (continued)

Column/Field	Description
	Ensure that you have the required ACF permissions to delete certificates from the archived inventory. For indicative instructions, see Deleting Individual Server Certificates from the Inventory and Deleting all Server Certificates. All user actions performed on or via the inventory are logged for auditing purposes.
	Use the archived certificates **Settings** to configure the behavior of the auto-archival and recovery features for archived certificates. Ensure that you have the required ACF permissions for configuring certificate archival settings. The instructions for configuring both features are covered in the Configuring Auto-Archival Settings and Recovering Archived Certificates sections.
	Use the **Columns** list to show/hide columns in the inventory. By default, the following columns are displayed: • **Common Name** • **Serial Number** • **Group** • **Issuer Common Name** • **Valid to (GMT)** • **Subject Alternative Names** • **Certificate Authority** • **Archive Reason** • **Archive Date** Ensure that you have the required ACF permissions to show/hide columns in the inventory.
	Use the pagination control dropdown to select the number of records that will be displayed per page of the inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Archived Certificates Inventory Structure (continued)

Column/Field	Description
	You can select to display 25, 50, 75, or 100 records per page of the inventory.
	Use the pagination navigation buttons to move between pages in the inventory.
	Use the **Refresh** button to reload the inventory to display the up-to-date records.

Configuring the Auto-Archival and Recovery Settings

Auto-archival of certificates esnures a clean active certificate inventory, minimizing manual overhead.

Ensure that you have the required ACF permissions for configuring certificate archival settings.

To configure the auto-archival rules and recovery behavior for certificates:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Archived Certificates**.
   The **Archived Certificates** inventory is displayed.
2. From the **Archived Certificates** inventory, click **Settings**.
   The **Settings** dialog box is displayed.
3. In the **Auto-Archival Rules** section:
   a. (Mandatory) From the **Auto-Archive When** field, select the certificate status values that should trigger automatic archival.
   b. In the **Auto-Archive After** field, enter the number of days after which automatic archival will be triggered, for the certificate status values selected in the above step.
4. In the **Recovery** section:

   a. To allow certificates to be moved back from the archived state to th monitored, select the **Recover archived certs as Monitored** checkbox.
   If this checkbox is not selected, the archived certificate is restored to its original state after recovery.

   b. From the **Recover To Group** field, to specify which certificate group the archived certificate will be moved to after recovery, select one of the following options :

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Default Group**

  Recovers the certificate and places it in the default group (restricted to admin access only)

- **Source Group** (default)

  Recovers the certificate and places it in the group from which it was originally archived

This behavior comes into effect when the Recover action is selected in the certificate inventory.

5. Click **Save**.
   The **Archival settings updated** confirmation message is displayed.

Recovering Archived Certificates

Ensure that you have the required ACF permissions to recover archived certificates.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Archived Certificates**.
   The **Archived Certificates** inventory is displayed.
2. From the **Archived Certificates** inventory, select the checkboxes corresponding to the certificate(s) you want to recover.
3. From the **Actions** dropdown menu, select **Recover**.
   The selected archived certificates are restored according to the recovery behavior configured here.

Certificate Reporting and Monitoring

Once the certificates in the infrastructure are discovered in AppViewX, they can be monitored as the reports in the Dashboards. In the dashboards, the user can track the certificates expiry, compliance, security details as the reports in the dashboard.

Reporting and monitoring the certificates are essential for an administrator to get complete visibility of all the certificates across multiple vendors and data centers in one single window pane. Certificates have a finite life span and are set to expire at different dates and times. Due to advancements in cryptography, there are high chances that the infrastructure will carry the weaker algorithm certificates which will be vulnerable to several attacks which will cause business outages. Using the dashboards and reports, the administrator can continuously monitor the status of the certificates in terms of expiry, security, compliance and so on.

- Accessing the Dashboard
- Creating a Dashboard
- Exporting Dashboard Information
- Importing a Dashboard

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Understanding Certificate Reports on the Dashboard
- Searching for Dashboard, Object, or Widget
- Deleting a Dashboard
- Insights
- Accessing the Discovery Summary Dashboard

Accessing the Dashboard

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. To go to the Dashboard inventory, from the top left corner of the screen, click **Dashboard**.

> **Note:** You can also click from the command bar.

The **Dashboard** page is displayed.

Dashboard page Actions

Options	Description
Search bar	Search using the required keyword(s) The research result is a list of items that match the specified keywords(s).
+	Allows users to create a **New** dashboard.
	Allows users to **Delete** a dashboard from the list.
	Allows users to **Export** a dashboard from the list.
	Allows users to **Import** a file to create a dashboard.
	Refresh the dashboard page
	Allows users to **Auto-sort** the dashboards alphabetically.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Creating a Dashboard

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. From the command bar on the top right corner of the page, click +.
   The **Create dashboard/widget** pop-up window is displayed.
3. In the **Create dashboard/widget** dialog box, enter or select the requested field information as described in the table below.

Field Description for Create dashboard/widget

Field	Description
***Dashboard name**	Enter the name of the dashboard.
***Select solution**	Select a solution from the options available in the dropdown.
***Widget type**	Select the type of the widget you want to create. The options are: • **Custom**: Select this option to create a customized Widget. • **Default**: Select this option to create a default Widget.
***Choose widgets**	Select the widget(s) from the options available in the dropdown. **Note:** This field is displayed only when you select **Widget type** as **Default**.
***Select widget**	Select the widget from the customized widgets displayed in the dropdown.
***Widget name**	Enter the name of the Widget.
Note: The asterisk (*) symbol indicates mandatory fields.	

4. Click **Create**.
   The dashboard is created.

Note: To discard the changes, click **Cancel**.

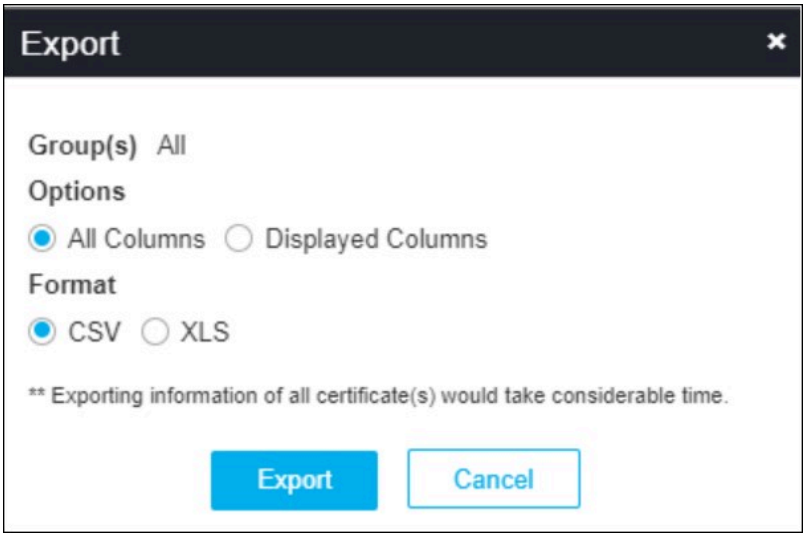
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Exporting Dashboard Information

You can export the dashboards in **.Cs** or **.json** format. The dashboards that are exported in the **.json** format can be imported to another build of the AppViewX platform.

To export dashboard information:

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. Select the dashboard to be exported and from the command bar at the top right corner of the screen, click the export icon.
   The **Export** pop-up window is displayed.



3. Select the required **Options** and **Format**.
   The selected dashboard(s) are exported to your local machine.

Importing a Dashboard

You can import the list of dashboards, which has the **Application View** widget. The import file must be in the **.text** and/or **.json** format and zipped.

To import a dashboard:

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The pinned or last viewed dashboard is displayed.
2. From the command bar at the top right corner of the dashboard page, click **Import**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Import** page is displayed.

3. Browse and open the dashboard import file in **.zip** format and click **Upload**.
4. Once the file is uploaded, click **Submit**.

   The selected dashboard(s) are imported to AppViewX platform.

Understanding Certificate Reports on the Dashboard

Certificate Reports give you visibility over all certificates and host information in the CERT+ inventory through different modes of discovery. With the available data, you can validate whether these certificates fall under the organization's security policy. CERT+ reports give insights on all important aspects of the product.

All these reports are categorized and available as multiple dashboards as default in AppViewX. Provided with that, custom dashboards with custom reports can also be created.

- Viewing Certificate Reports
- Default Reports
- Understanding the Server Certificate Dashboard
- Understanding the Client Certificate Dashboard
- Report by Certificate Authority
- Understanding the Code Signing Dashboard
- Stale Certificate Report
- Count of issuer
- Server Certificate Security Dashboard
- Understanding the Client Certificate Security Dashboard
- Understanding the Server Endpoint Security Dashboard
- Understanding the Client Endpoint Security Dashboard
- Understanding the Server Standard Dashboard
- Understanding the Client Standard Dashboard
- Understanding the Trust Store Certificates Dashboard
- Report Customization
- Security Posture Determination and Interpretation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- License Report
- Discovery

Viewing Certificate Reports

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > <type of certificate you want the reports for>.
   The certificate inventory page, for the selected certificate type, is displayed.
2. From the top right corner of the page, click the **Reports** toggle.
   Reports for selected certificate type are displayed.

Although each certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets in the report:

- **Report by Certificate Authority -** A bar chart that shows the total certificate count for each Certificate Authority (CA), made up of colored bars representing the following statuses:
  - Green - Valid certificates
  - Blue - Certificates with an expiry in 90 days
  - Yellow - Certificates with expiry in 30 days
  - Orange - Certificates with expiry in 10 days
  - Red - Expired certificates
  - Black - Revoked certificates
  - Gray - New certificates
- **Expiry Report by Month -** A bar chart that shows the total number of certificates expiring each month.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Policy Compliance -** A pie chart that shows the number of compliant and non-compliant certificates in the system, with each sector in the chart representing a different kind of policy such as Strict or Suggestive. You can also export the report details from the Policy Compliance Report widget.
- **Stale Certificate -** A pie chart that shows the number of expired and revoked certificates.
- **Certificate Summary -** A doughnut chart that categorizes the certificates based on expiration, with the total count of certificates made up of colored bars representing the same statuses listed for the Report by Certificate Authority widget. You can also configure the report settings from the Certificate Summary Report widget.
- **Count by Issuer -** A doughnut chart that shows the total number of certificates managed by the issuer such as Root CA or the Intermediate CA. You can also configure the report settings from the Count by Issuer widget.

Default Reports

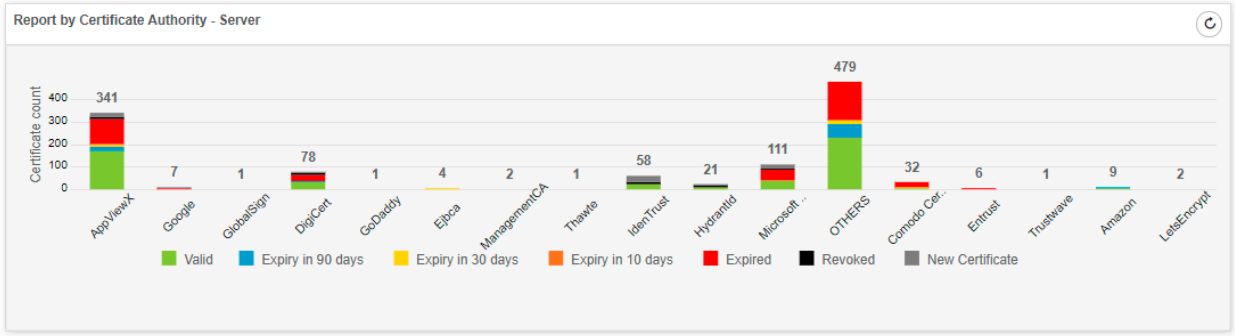
AppViewX CERT+ has a few in-built reports (recommended) that are available as default reports. These reports can be triggered directly to take necessary actions. The primary risk to be addressed is to enforce security compliance. Compliance reports that are provided as in-built reports can be used to categorize certificates based on the non-compliant parameter. This information (value addition) can be used to enforce the application team to onboard for automation.

Understanding the Server Certificate Dashboard

The certificates from the Server inventory will be shown in this dashboard as the following reports:

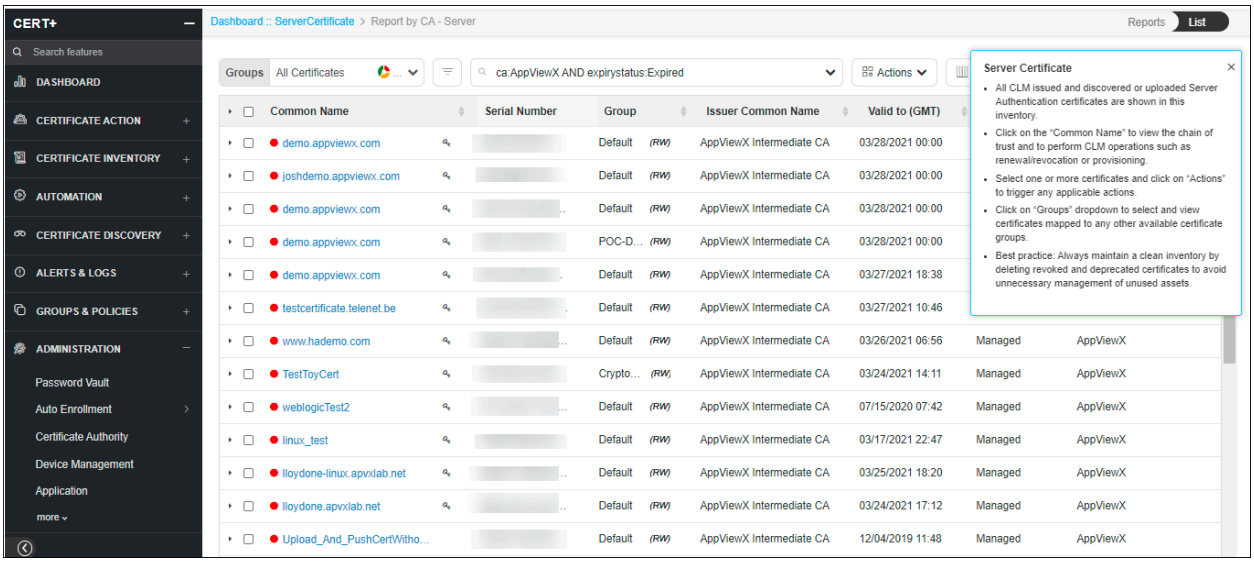
Report by Certificate Authority - Server

This report shows the count of certificates in the server inventory with respect to the certificate authorities and the expiry information.



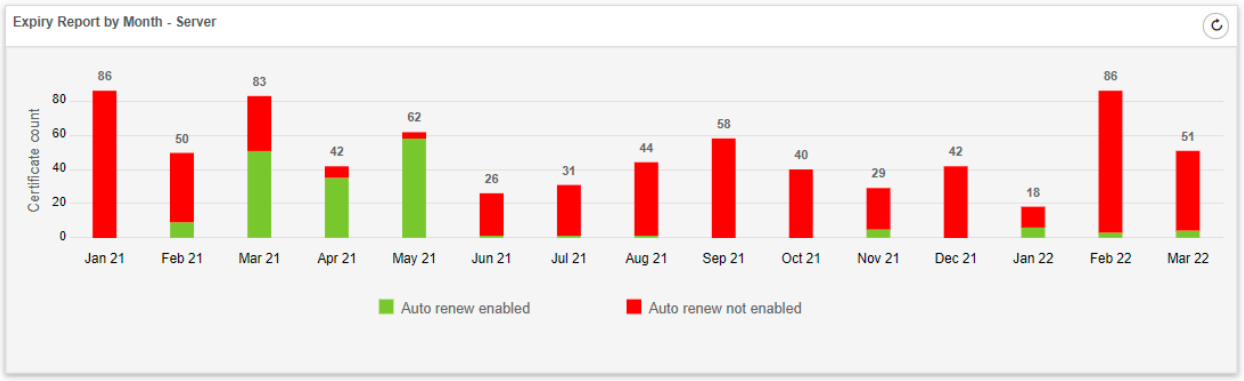
On click of any of the bar of this report, the filtered inventory view will be shown as below to proceed any further actions:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



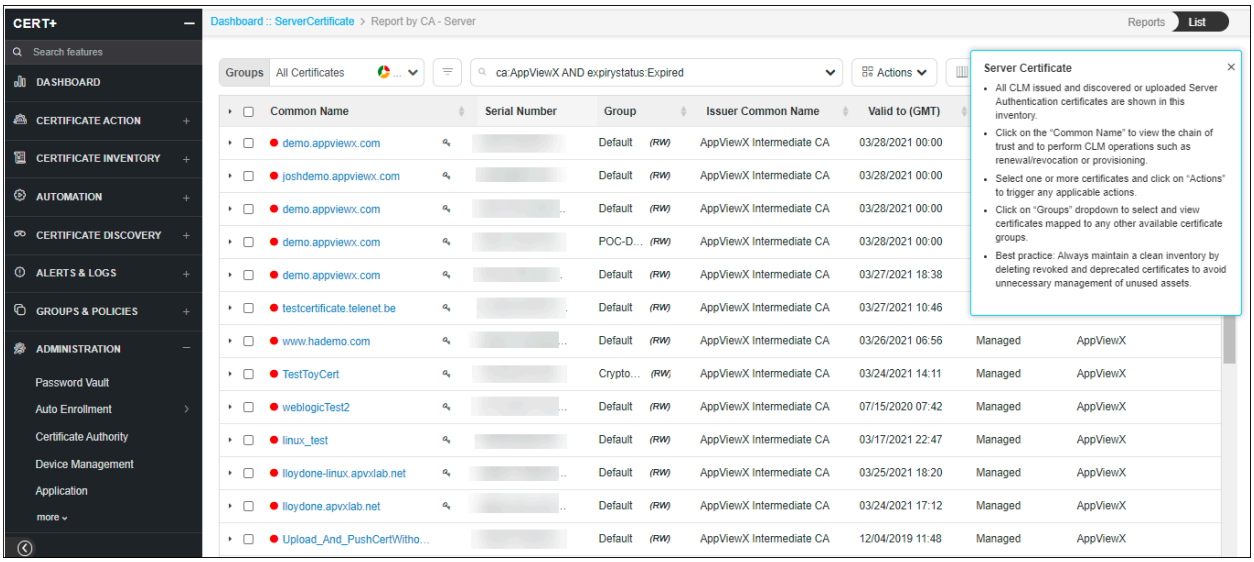
Expiry Report by Month

This report shows the count of certificates with respect to expiry month information.



On click of any of the bar, the filtered certificates inventory will be shown as below to perform any inventory actions:

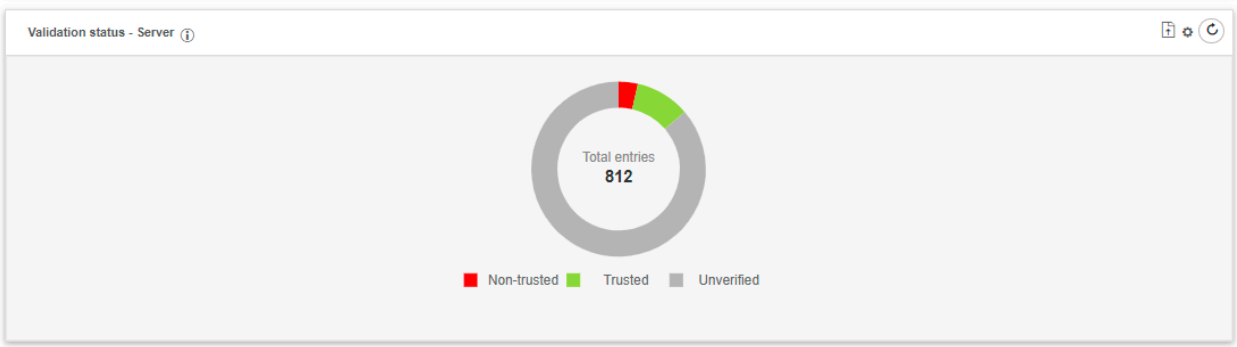
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Validation Status

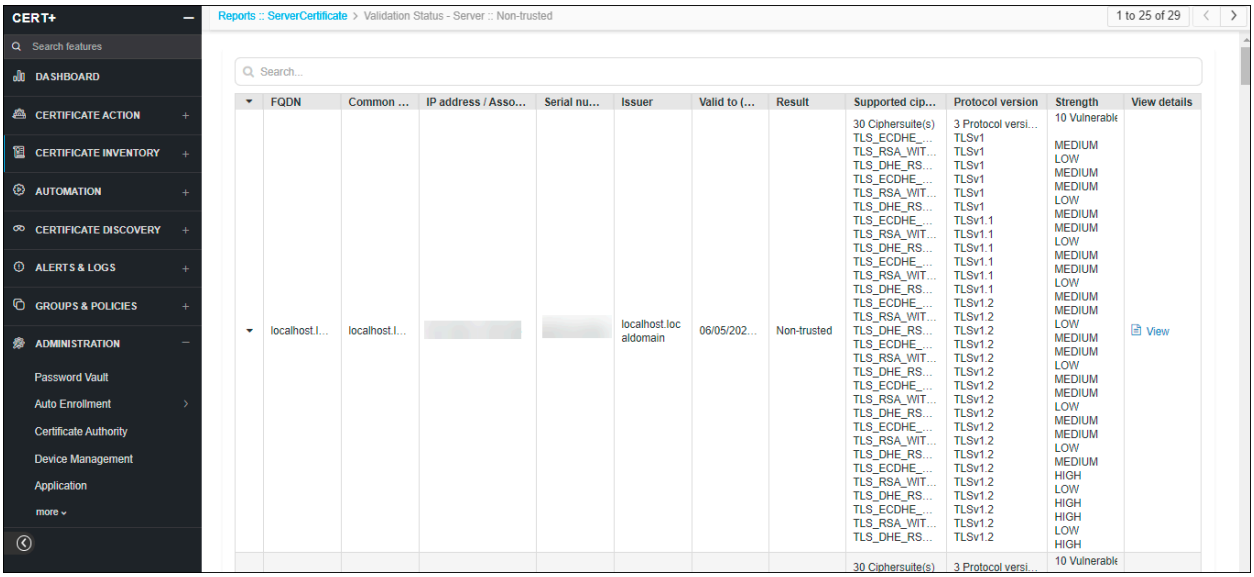
This report shows the count of server certificates with respect to the following:

- Trusted – When the chain of trust can be formed with the end server certificate it will be categorized as a trusted certificate.
- Non-trusted – When the chain of trust cannot be formed with the end server certificate it will be categorized as non-trusted.
- Unverified – When the server certificates are yet to be taken for validation, they will be categorized as unverified.



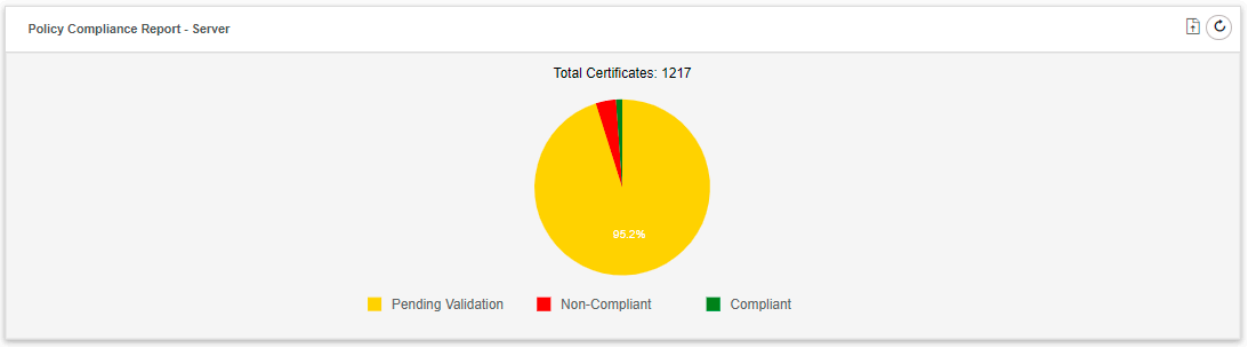
When a section of this pie chart is clicked, the corresponding filtered certificate data is displayed, as shown in the image below:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



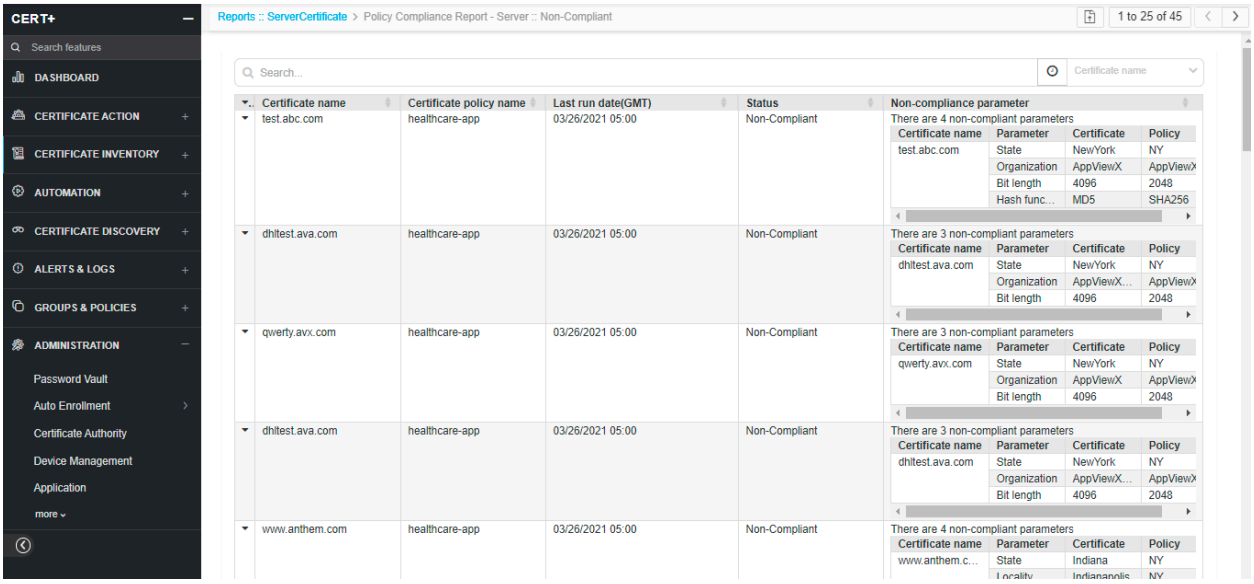
Policy Compliance Status

This report shows the count of server certificates as compliance or non-compliance based on the certificate group policy associated with the certificates.



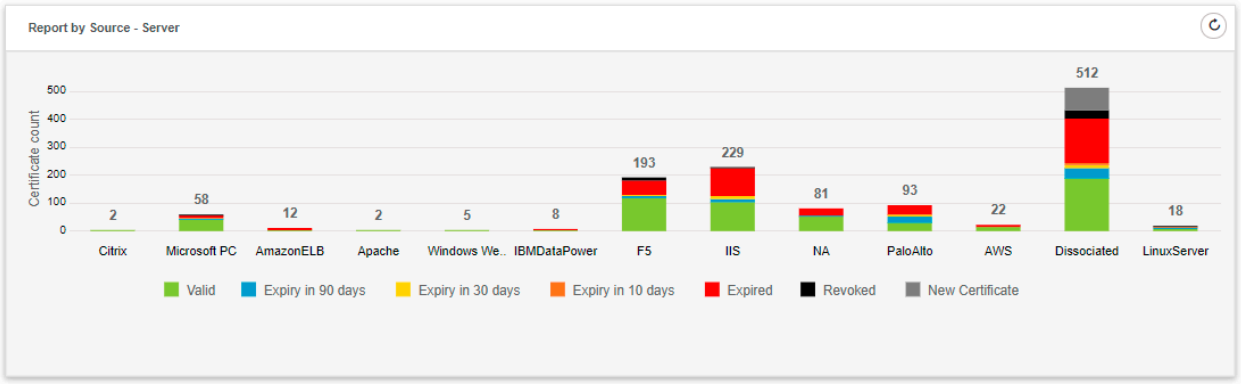
When a section of this pie chart is clicked, the corresponding filtered certificate data is displayed, as shown in the image below:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



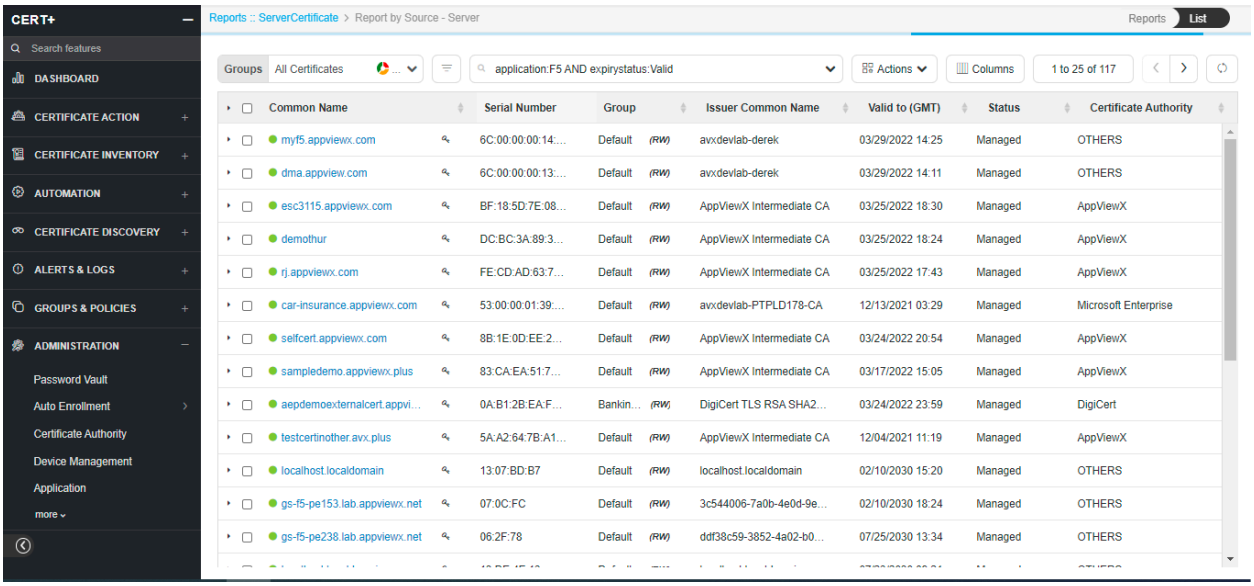
Report by Source

This report shows the count of server certificates with respect to the source from where the certificates are discovered along with the expiry status.



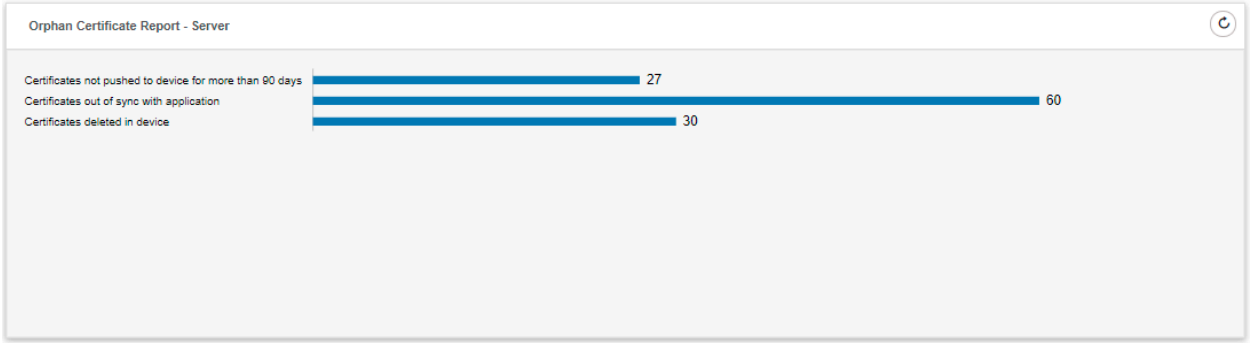
On click of anywhere in the bar chart, the filtered certificates data will be shown as below:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



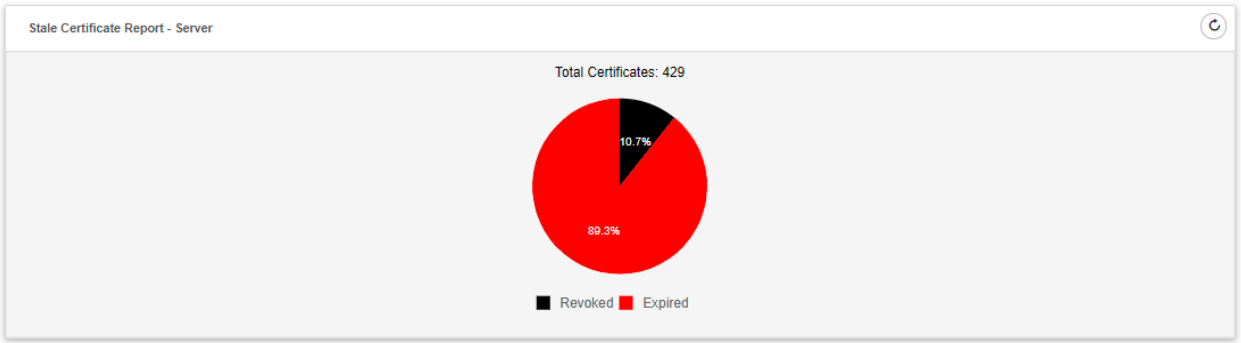
Orphan Certificate Report

This report shows the count of server certificates that are not associated/installed in any device/server.



Stale Certificate Report

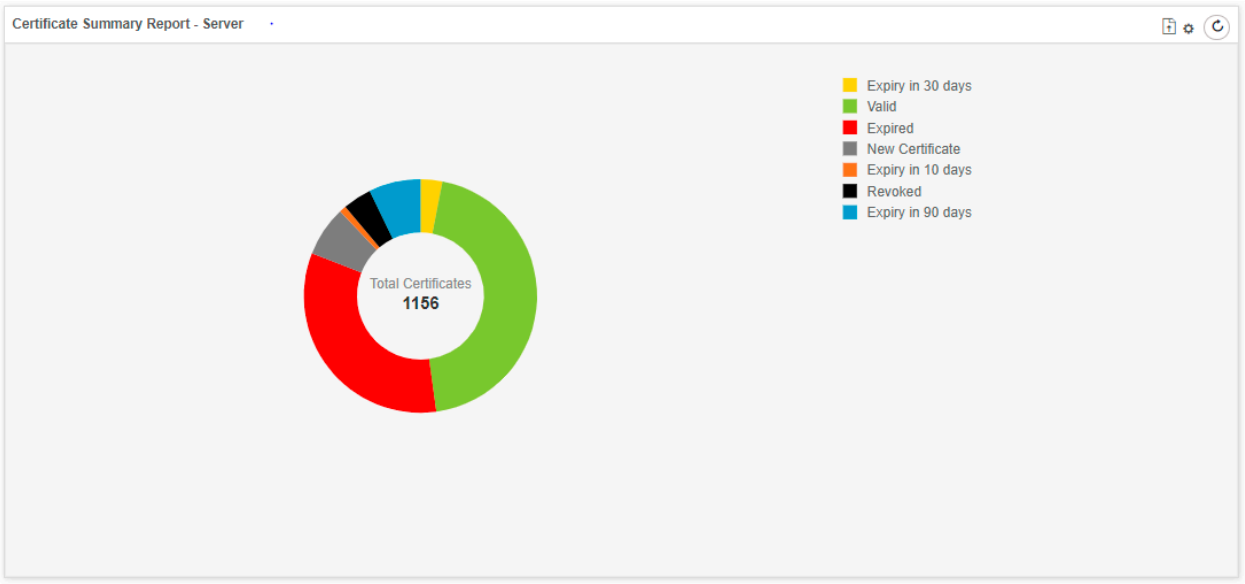
This report shows the count of server certificates that are either revoked or expired.



Certificate Summary Report

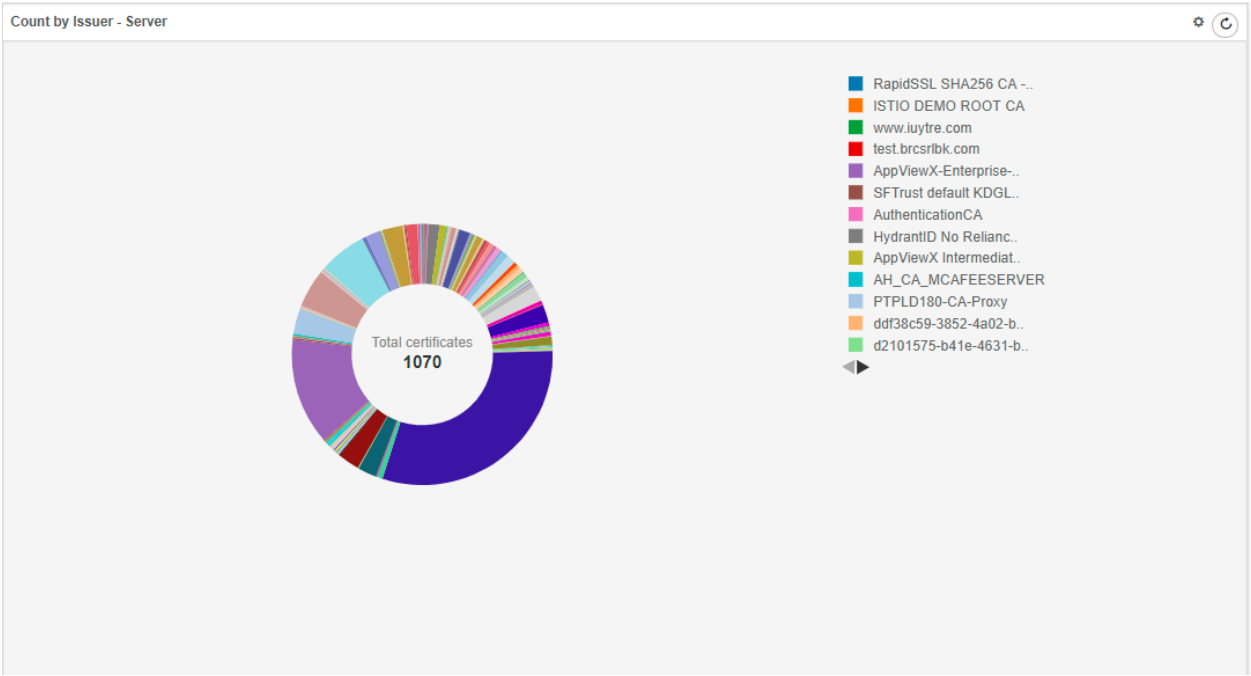
This report shows the count of certificates with respect to their expiry status.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Count by Issuer

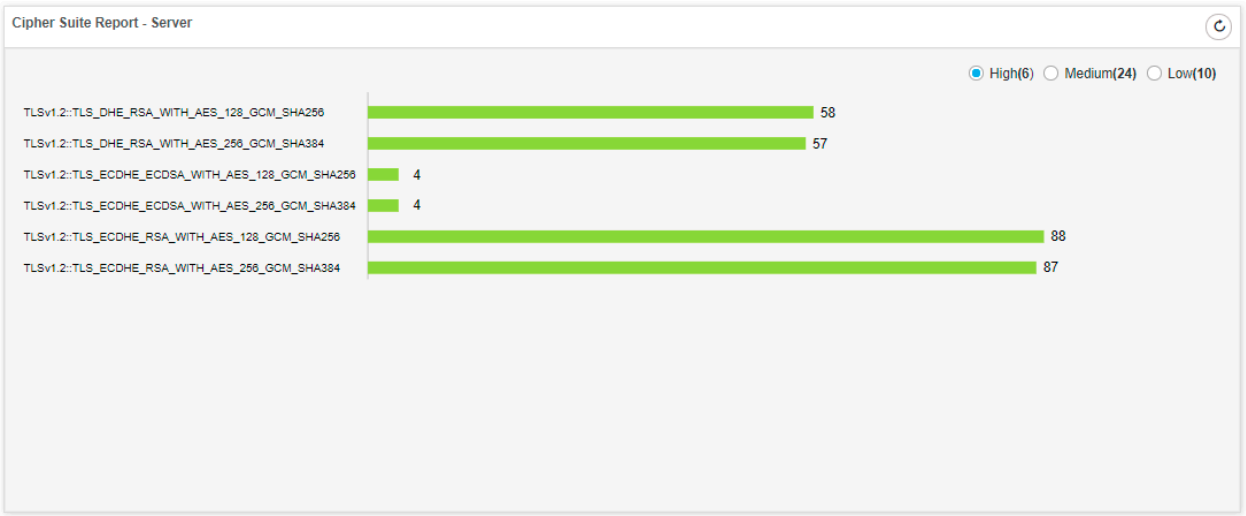
This report shows the count of certificates with respect to the issuer details.



Cipher Suite Report

This report shows the count of certificates with respect to the cipher suites. They are also categorized as Low, Medium, and High based on the cipher suites.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

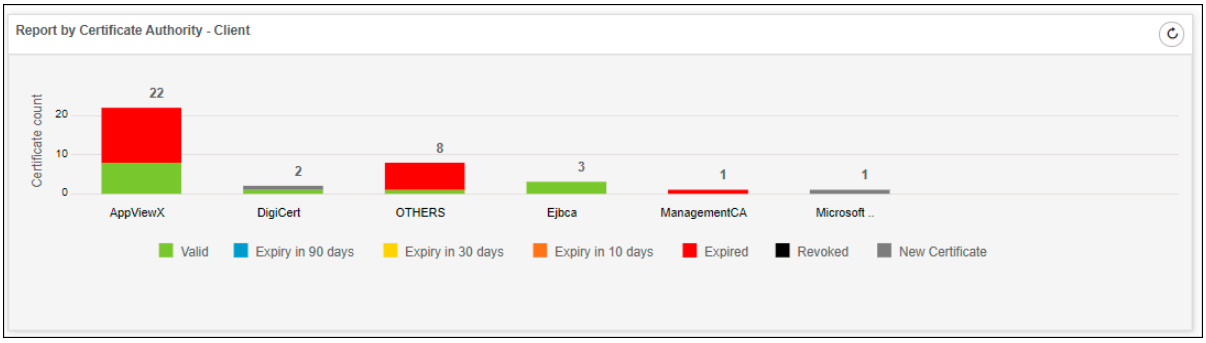


Understanding the Client Certificate Dashboard

This dashboard displays reports related to the certificates from the Client certificate inventory. You can also access this dashboard from the **Client Certificate** inventory page, by selecting **Reports** in the toggle at the top right corner of the page.

Report by Certificate Authority - Client

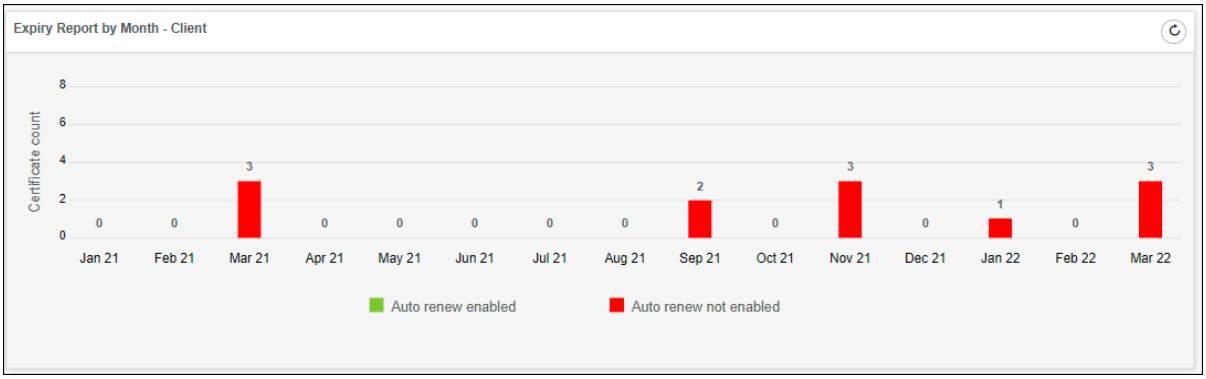
This report shows the count of certificates in the client inventory with respect to the certificate authorities and the expiry information.



Expiry Report by Month - Client

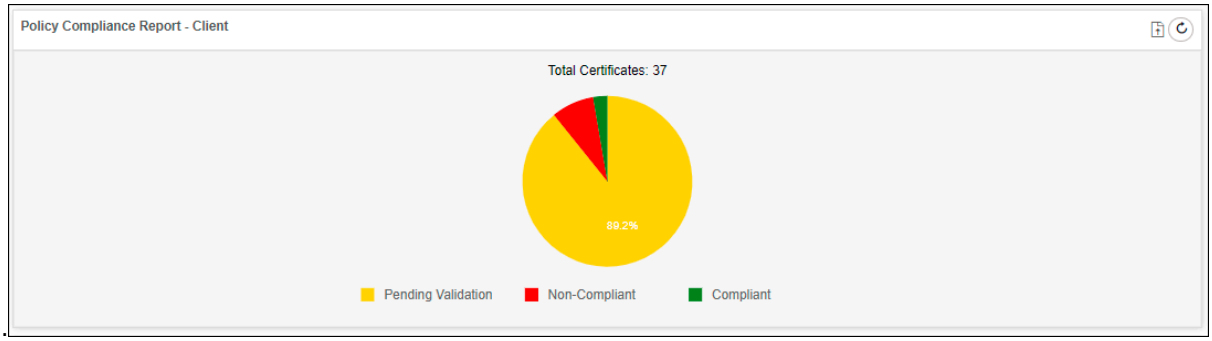
This report shows the count of certificates with respect to expiry month information.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



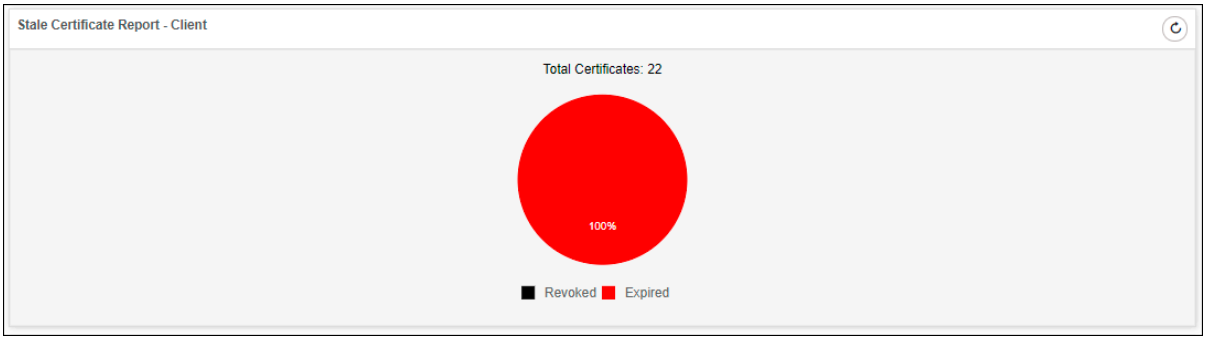
Policy Compliance Report - Client

This report shows the count of client certificates as compliant or non-compliant based on the group policy assigned to the certificate.



Stale Certificate Report - Client

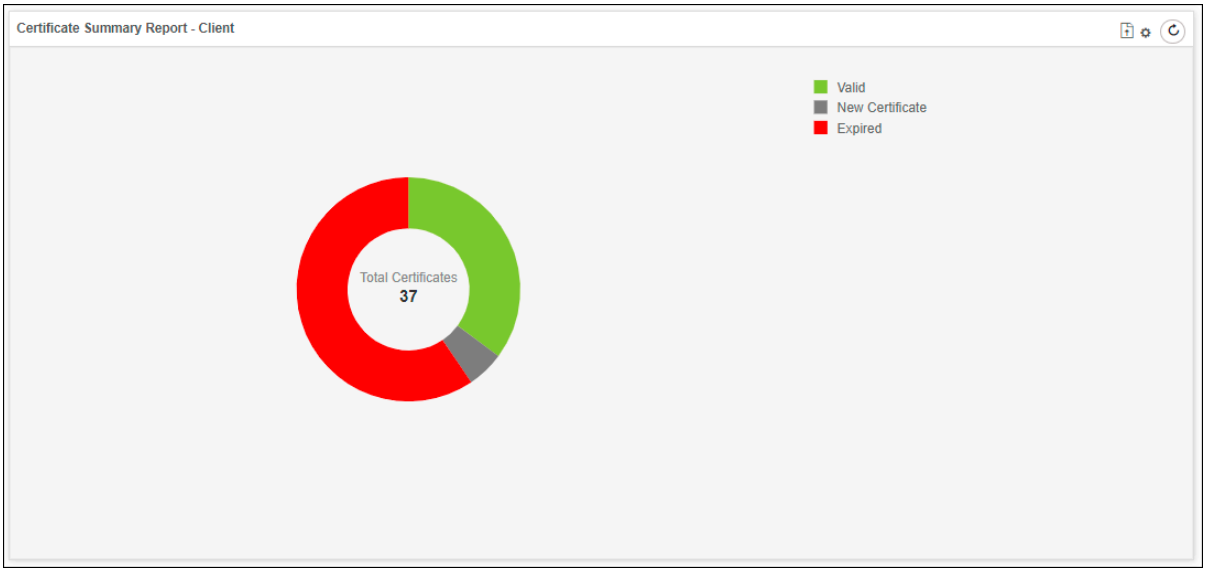
This report shows the count of client certificates that are either revoked or expired.



Certificate Summary Report - Client

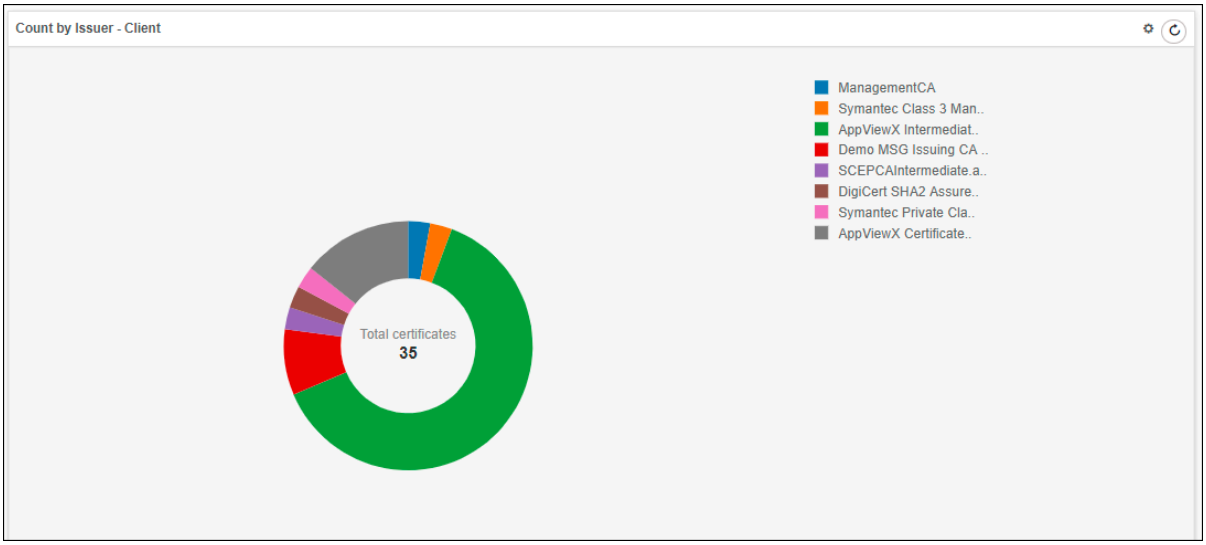
This report shows the count of certificates with respect to their expiry status.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Count by Issuer - Client

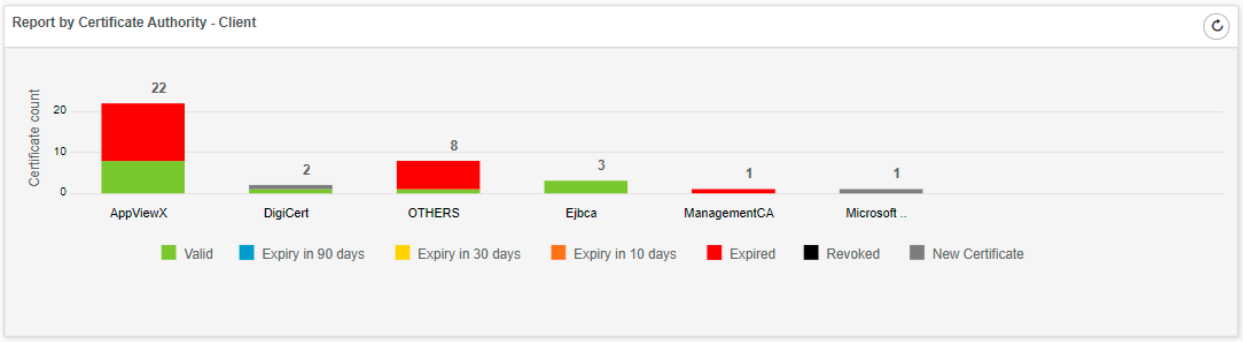
This report shows the count of client certificates with respect to the issuer details.



Report by Certificate Authority

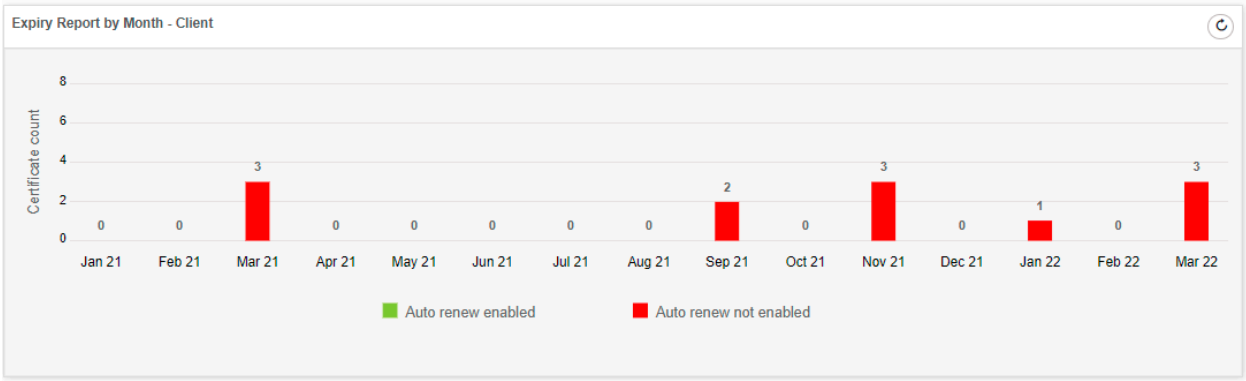
This report shows the count of certificates in the client inventory with respect to the certificate authorities and the expiry information.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



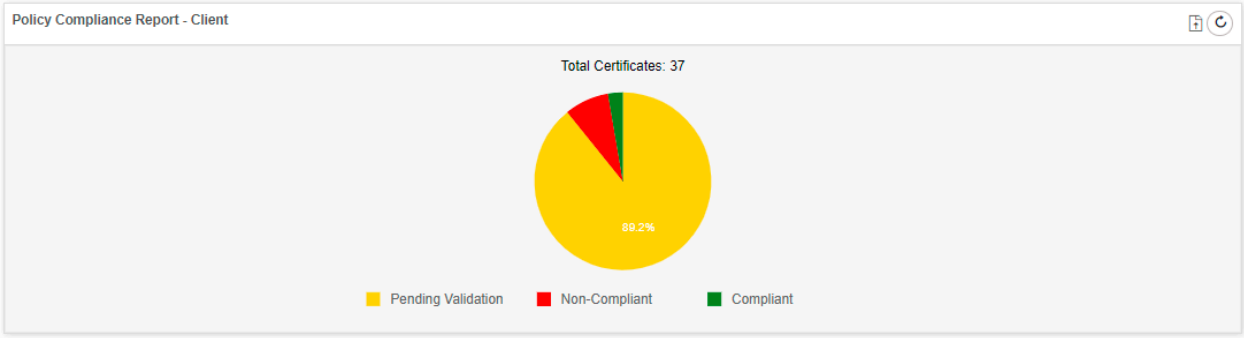
Expiry Report by Month

This report shows the count of certificates with respect to expiry month information.



Policy compliance status

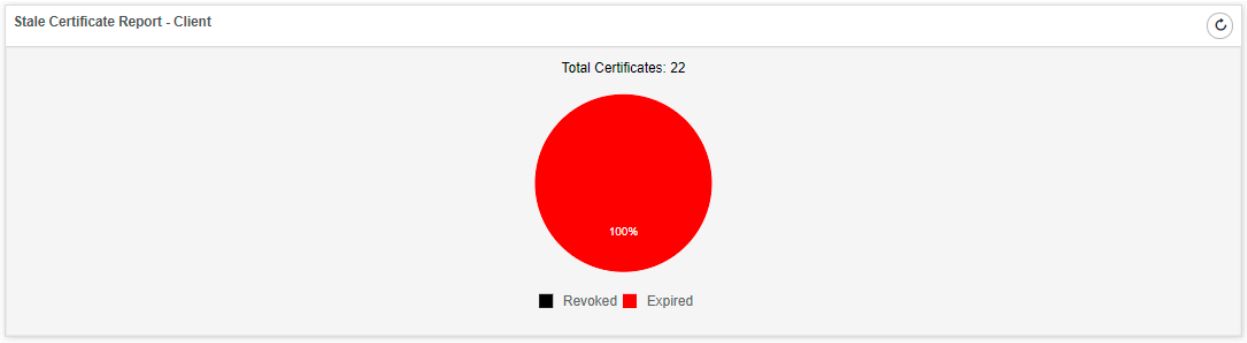
This report shows the count of client certificates as compliance or non-compliance based on the group policy assigned to the certificate.



Stale certificate report

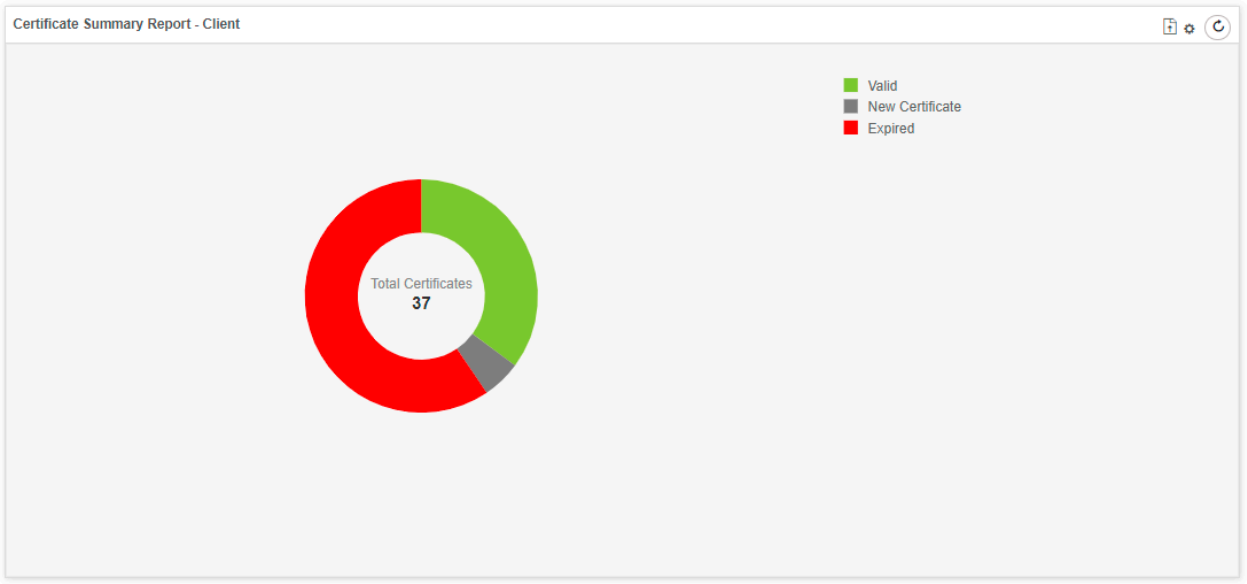
This report shows the count of client certificates that are either revoked or expired.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Certificate Summary Report

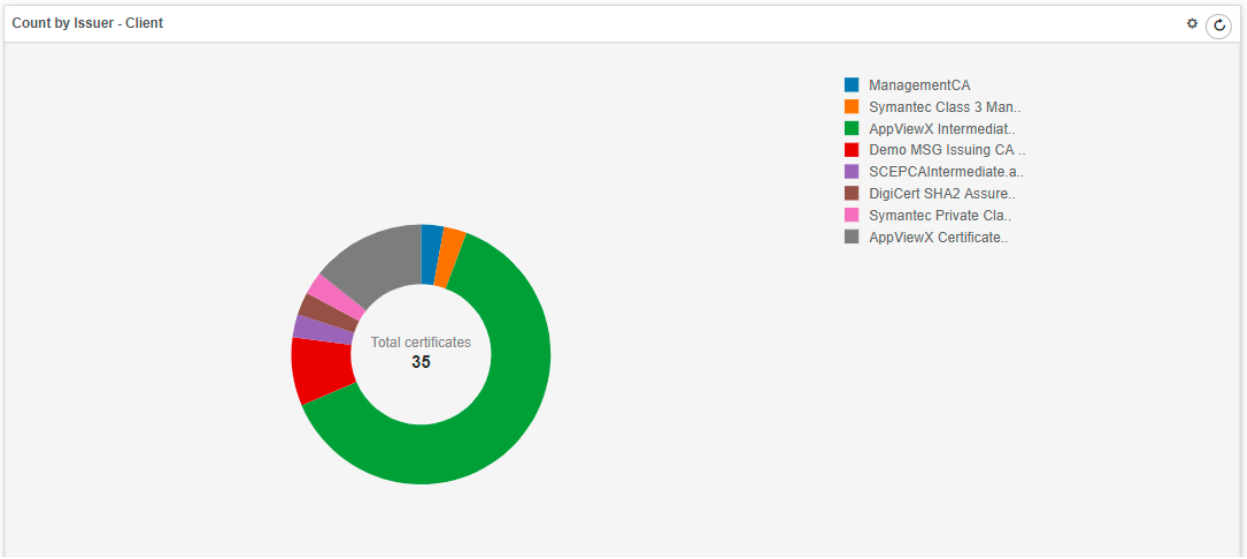
This report shows the count of certificates with respect to their expiry status.



Count of issuer

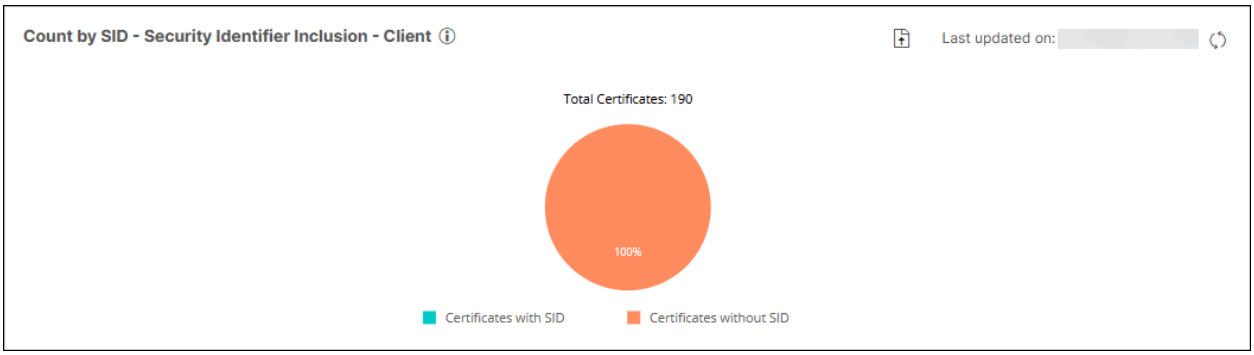
This report shows the count of client certificates with respect to the issuer details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Count by SID Report

This report shows the certificate count for certificates with and without an SID. A Security Identifier (SID) is a unique, immutable identifier assigned by Windows to each security principal.



The report uses a pie chart widget to show certificates with and without an SID.

The following certificates qualify as certificates with an SID:

- Certificates with the SID present in other extensions
- Certificates with the SID in the SAN (URI as well as other name) and having the following OIDs:
  - **1.3.6.1.4.1.311.25.2**
  - **1.3.6.1.4.1.311.25.2.1**

The (**Export** icon can be used to export the report as a **.csv** file.

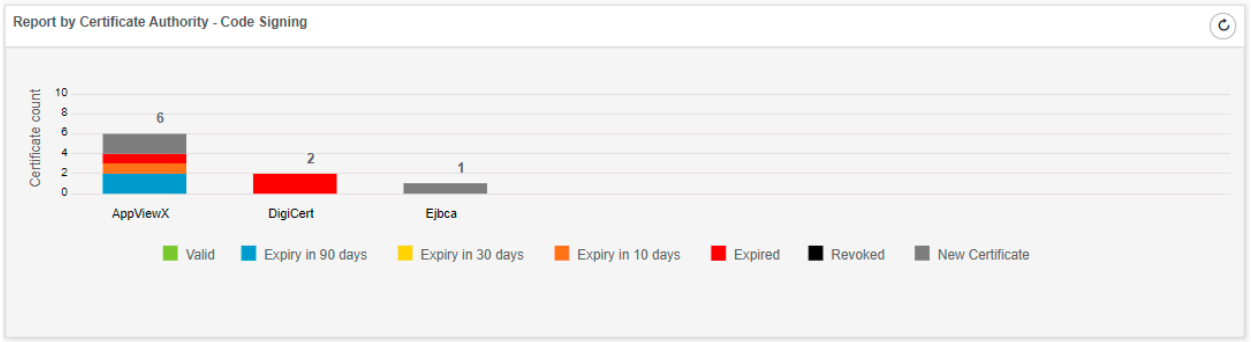
To be redirected to the certificate inventory filtered for certificates with/without the SID, click the corresponding pie slice.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To hide the representation of certificates with/without an SID, click the corresponding legend. To unhide it, click the corresponding legend again.

Report by Certificate Authority

This report shows the count of certificates in the code signing inventory with respect to the certificate authorities and the expiry information.



Understanding the Code Signing Dashboard

This dashboard displays reports related to the certificates from the Code Signing certificate inventory. You can also access this dashboard from the **Code Signing Certificate** inventory page, by selecting **Reports** in the toggle at the top right corner of the page.

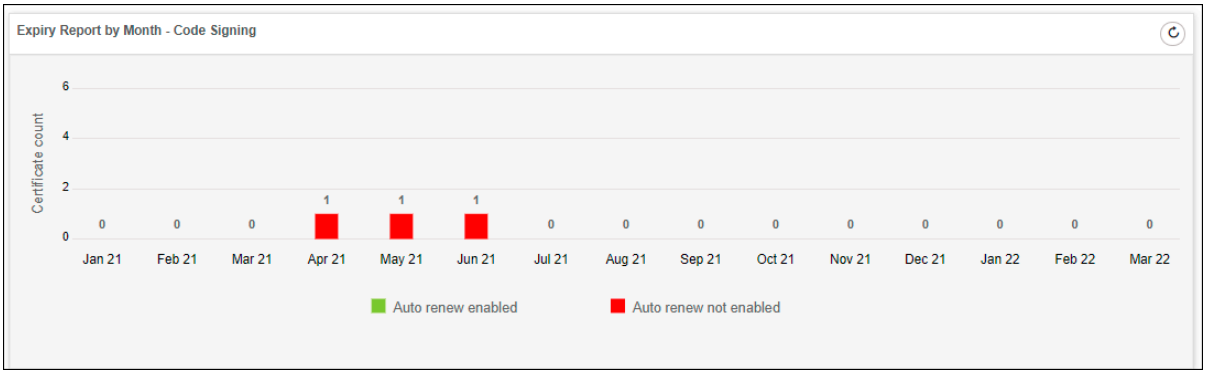
Report by Certificate Authority - Code Signing

This report shows the count of certificates in the code signing inventory with respect to the certificate authorities and the expiry information.

Expiry Report by Month - Code Signing

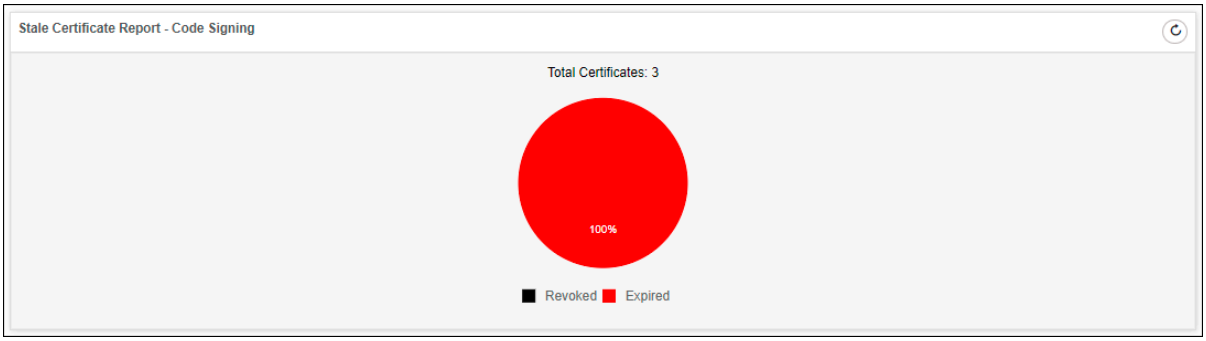
This report shows the count of code signing certificates with respect to expiry month information.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



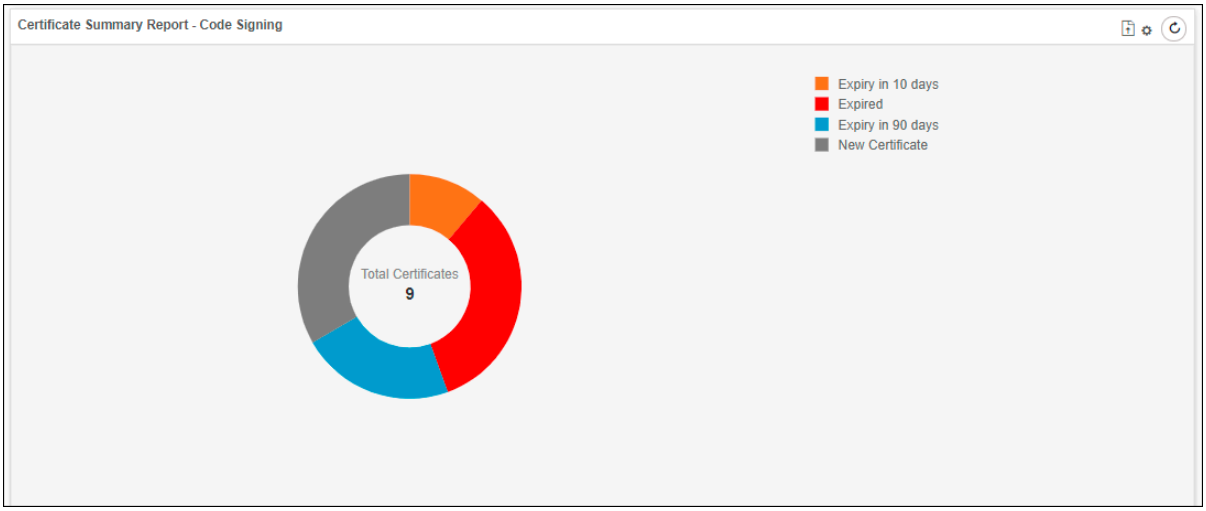
Stale Certificate Report - Code Signing

This report shows the count of code signing certificates that are either revoked or expired.



Count by Issuer - Code Signing

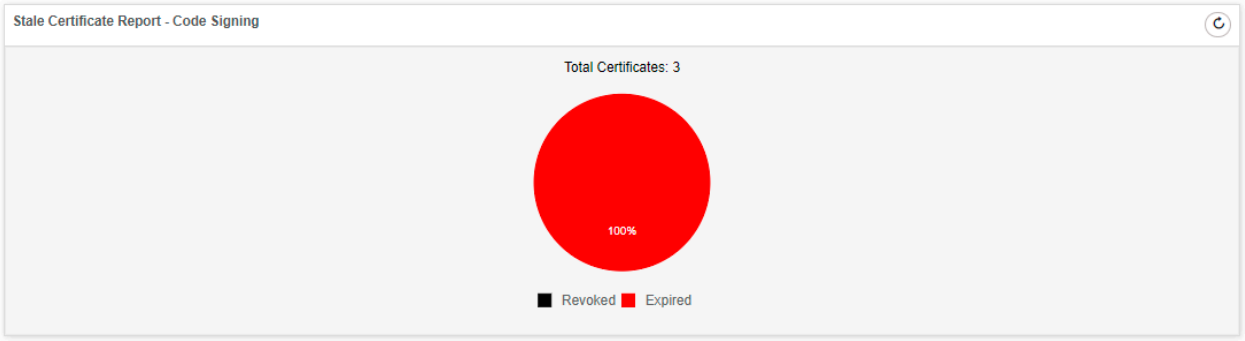
This report shows the count of client certificates with respect to the issuer details.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

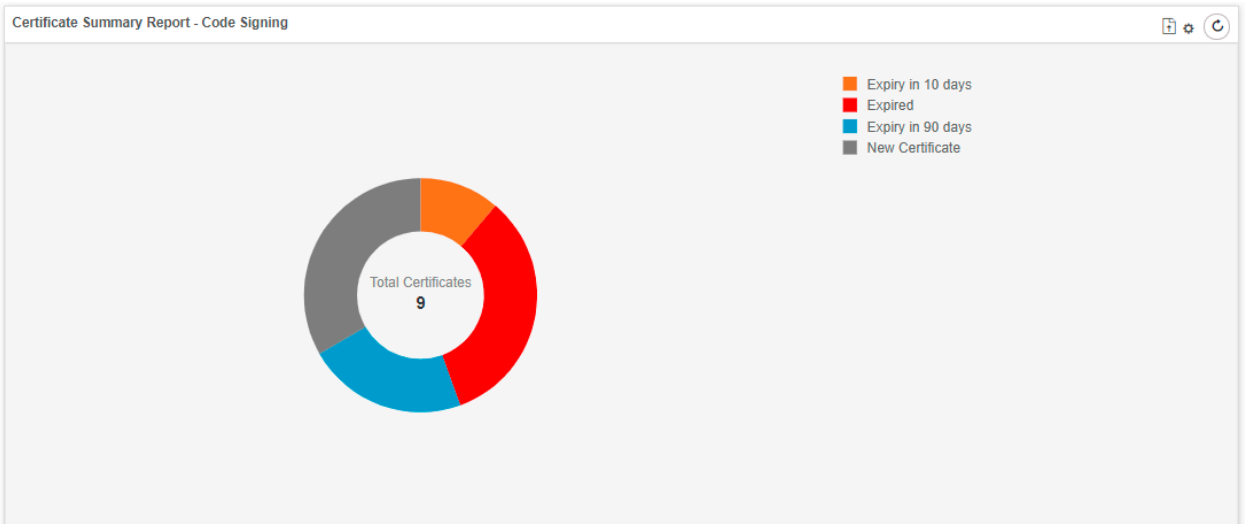
Stale Certificate Report

This report shows the count of code signing certificates that are either revoked or expired.



Count of issuer

This report shows the count of client certificates with respect to the issuer details.



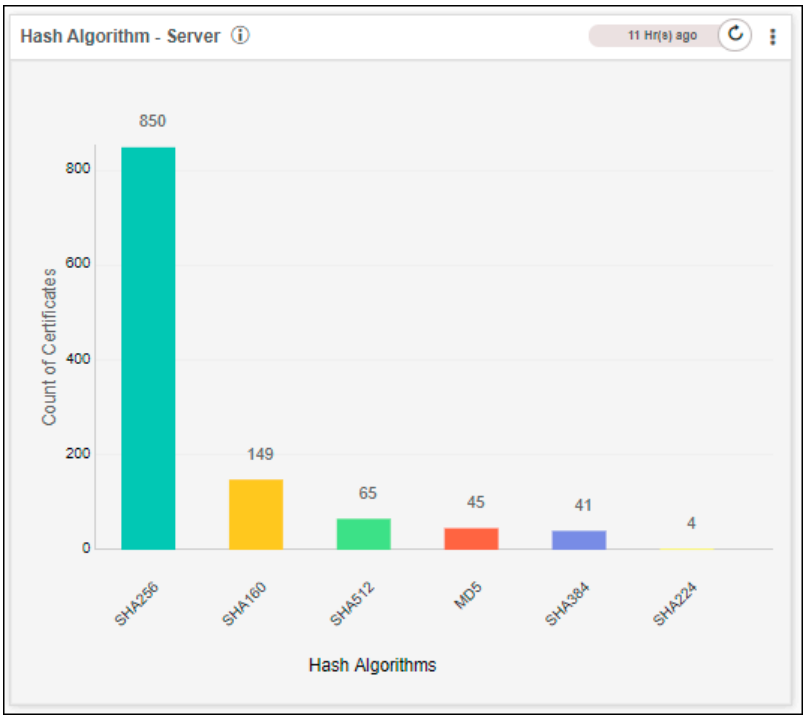
Server Certificate Security Dashboard

For the certificates in the Server inventory, this dashboard displays the following reports:

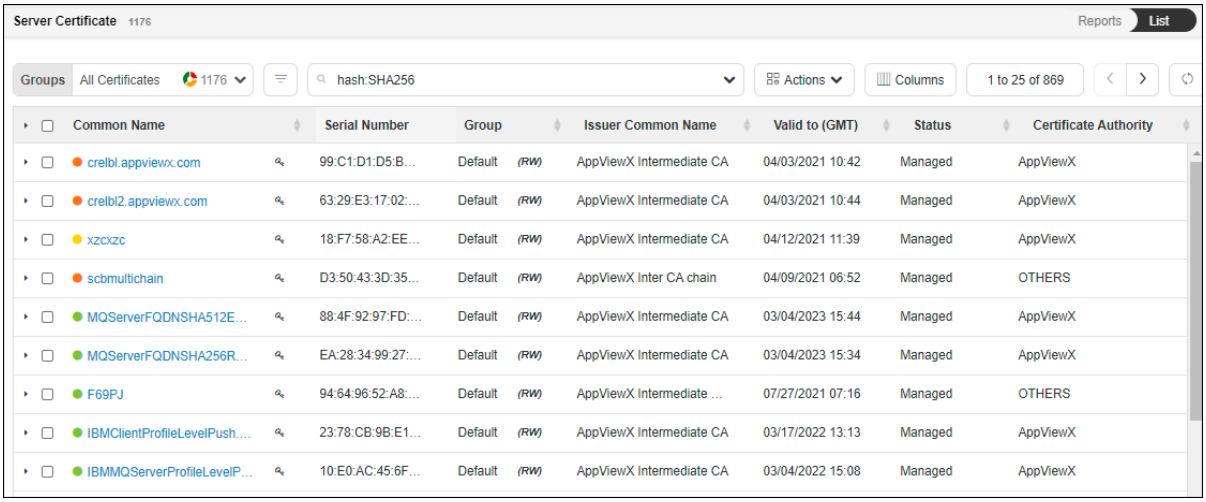
Hash Algorithm - Server

This report shows the count of certificates with respect to the hash algorithm available in the server inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



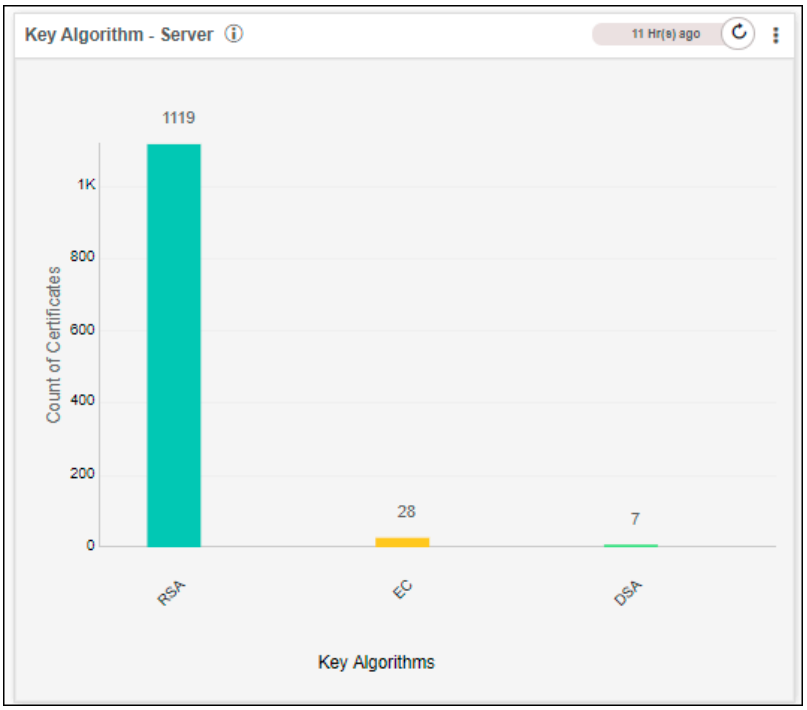
On clicking any bars of the report, the filtered data of certificates is displayed.



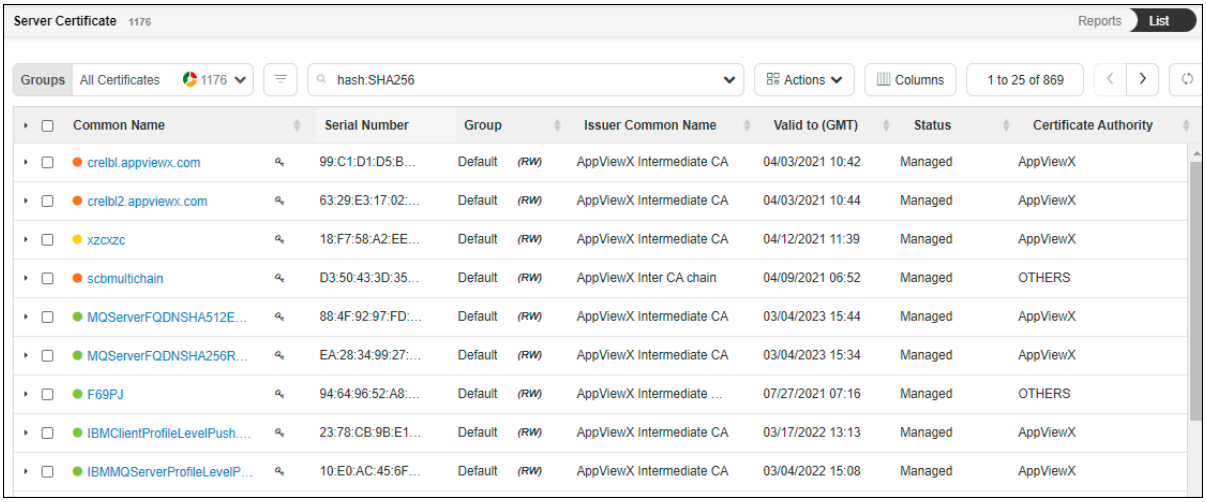
Key Algorithm - Server

This report shows the count of certificates with respect to the key algorithms available in the server inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



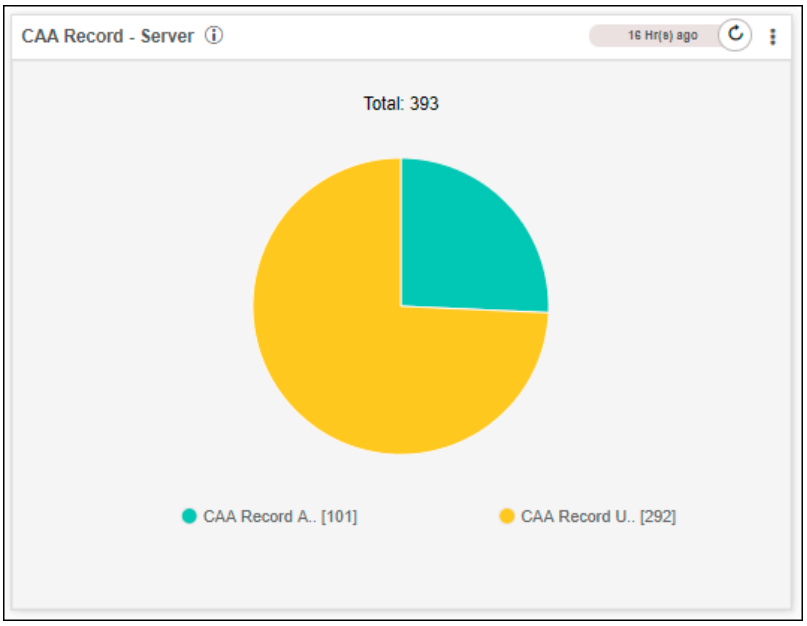
On clicking any bars of the report, the filtered data of certificates is displayed.



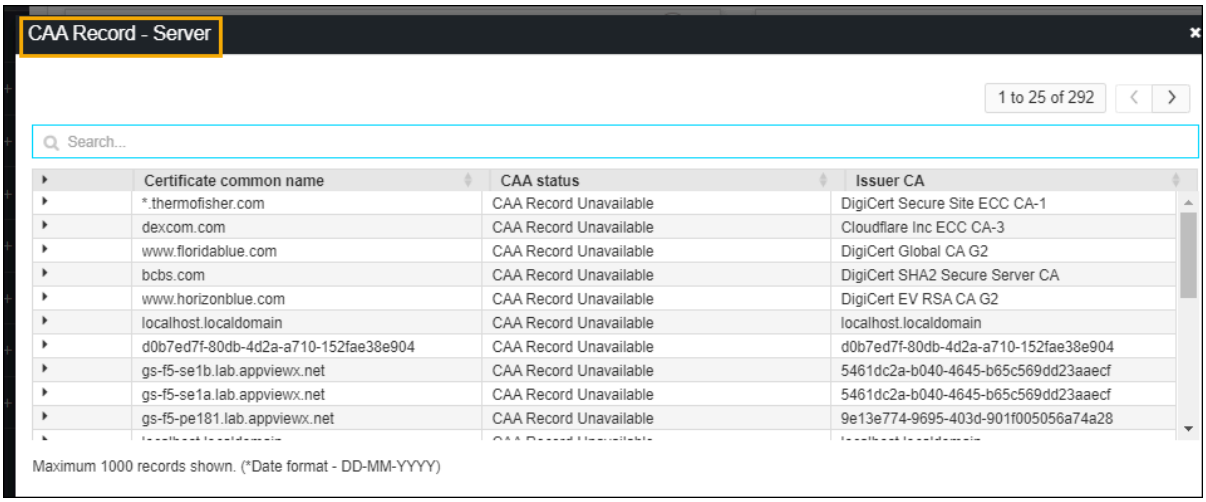
CAA Record - Server

This report shows the count of certificates with and without CAA records in the server inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



On clicking any parts of the report, the filtered data of certificates is displayed.

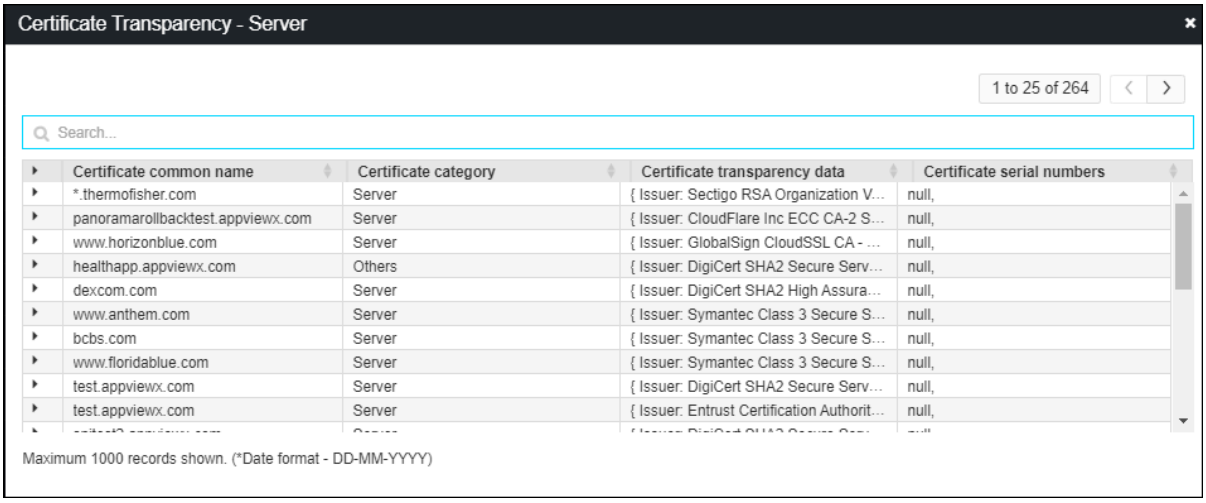


Certificate Transparency - Server

This report shows the count of application/FQDNs for which more certificates are available and only a few are managed/monitored in server certificate inventory. Currently the report is disabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

On clicking any parts of the report, the filtered data of certificates is displayed.



Understanding the Client Certificate Security Dashboard

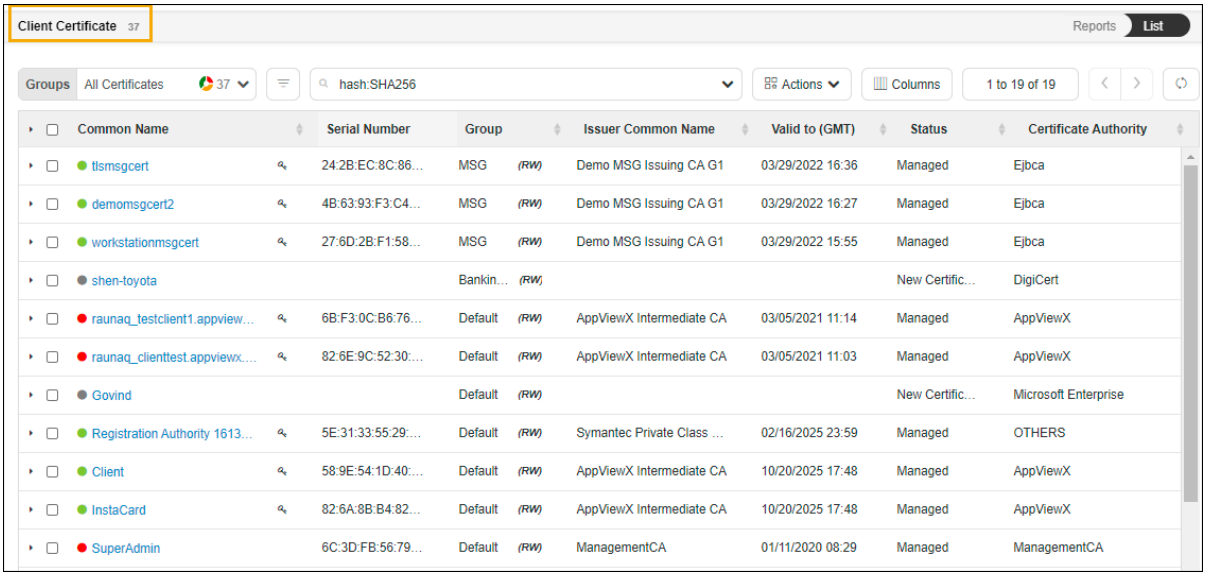
For the certificates in the Client inventory, this dashboard will be shown as the reports:

Hash Algorithm - Client

This report shows the count of certificates with respect to the hash algorithm available in the Client inventory.

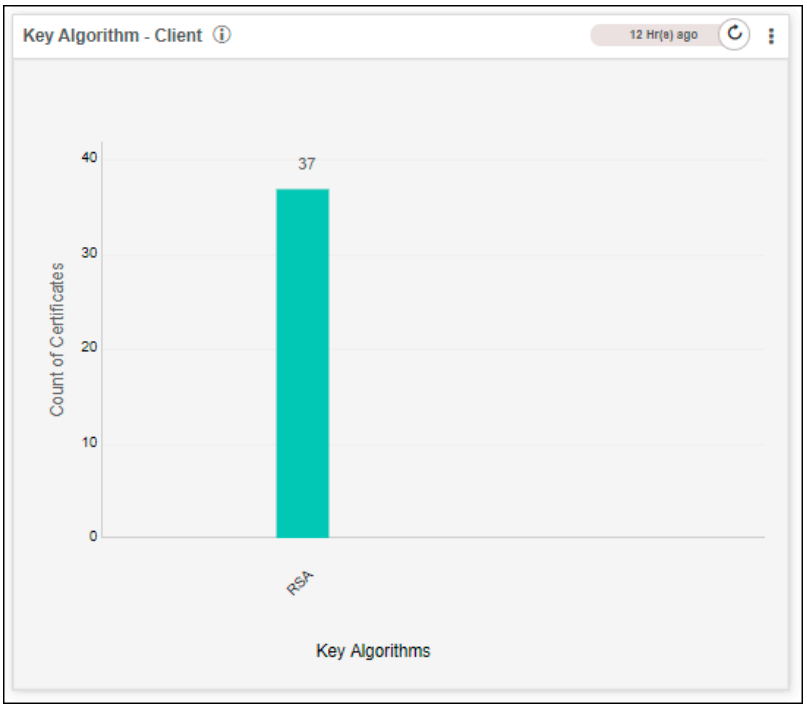
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

On clicking any bars of the report, the filtered data of certificates is displayed.



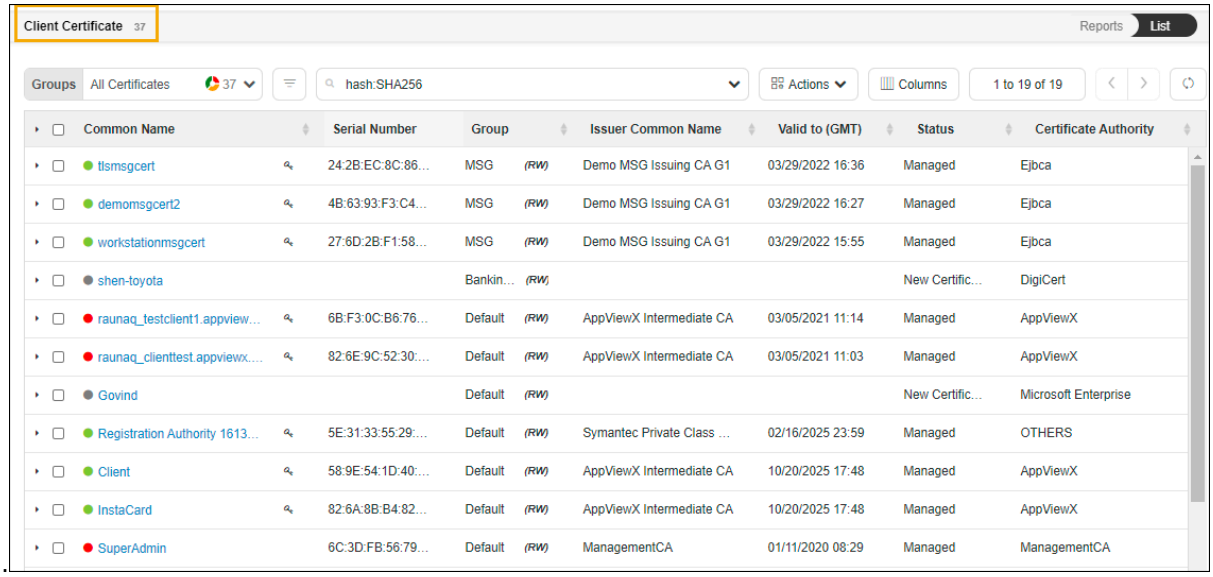
Key Algorithm - Client

This report shows the count of certificates with respect to the key algorithms available in the Client inventory.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

On clicking any bars of the report, the filtered data of certificates is displayed.

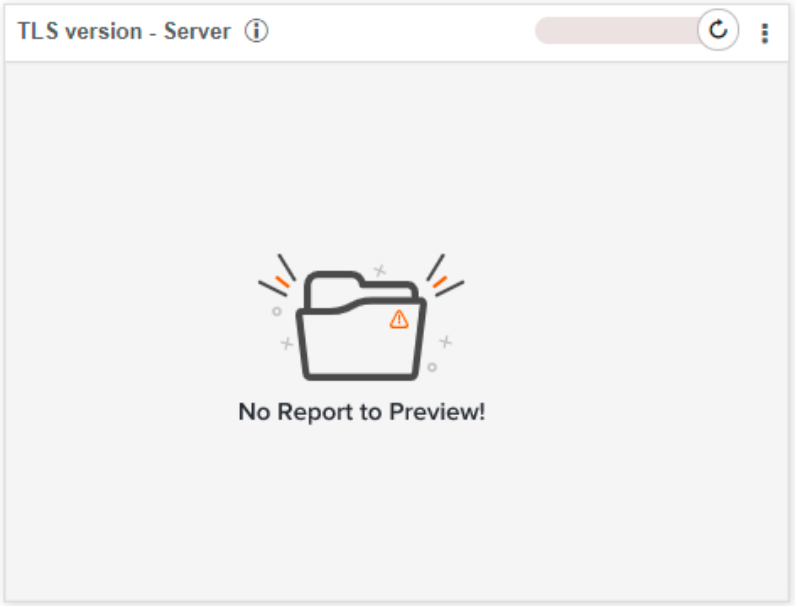


Understanding the Server Endpoint Security Dashboard

For the certificates in the Server inventory which are associated with the endpoints, from a security perspective, the following reports are available:

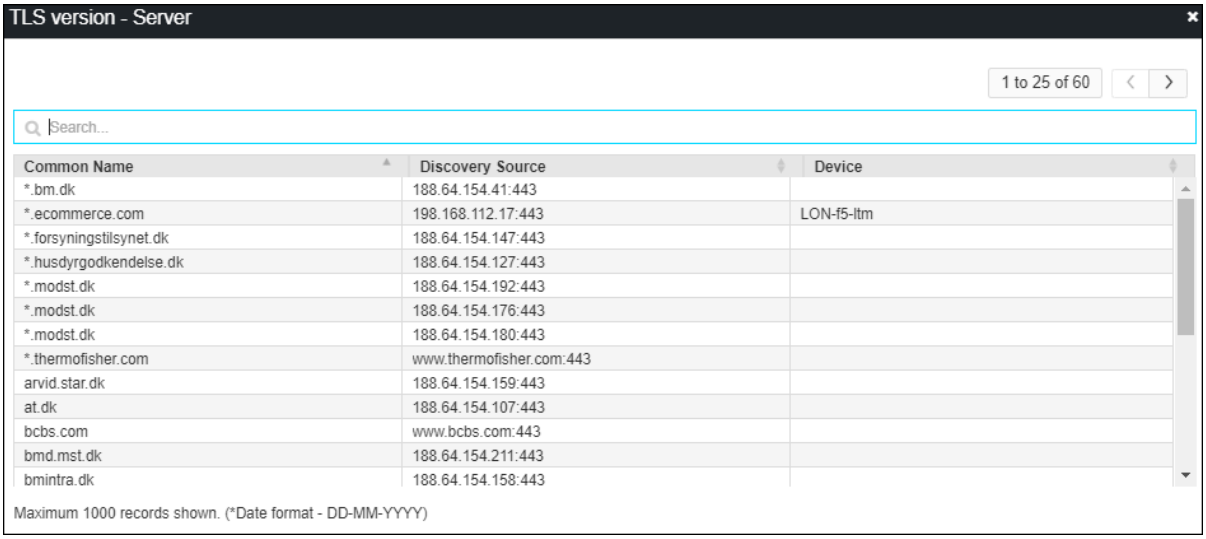
TLS Version - Server

This report shows the count of certificates with respect to the TLS versions available in the server inventory.



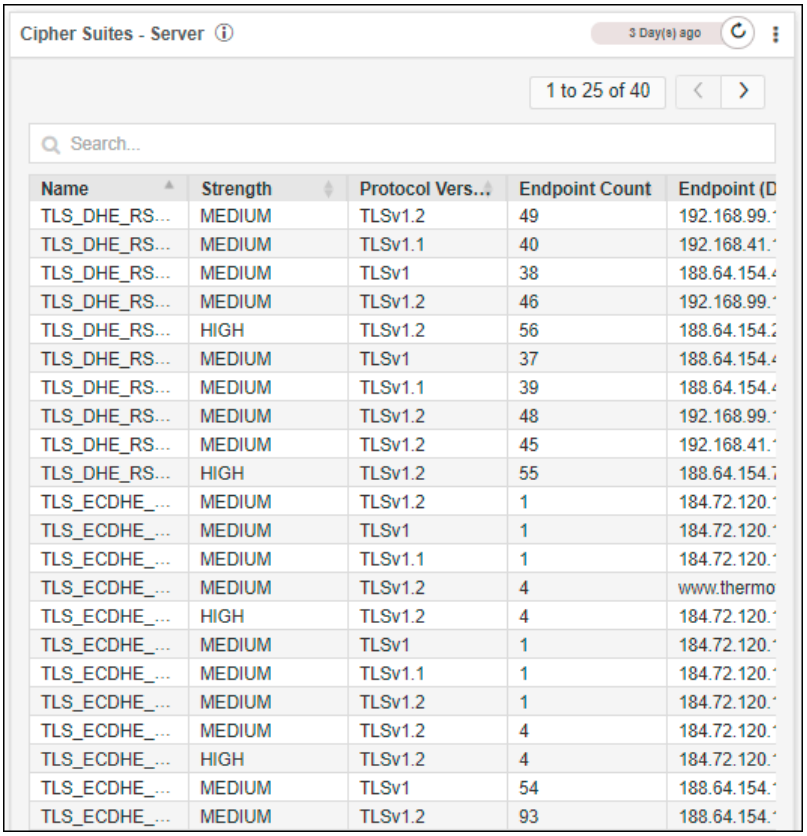
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Clicking the **Endpoint Count** value in the report displays the respective data of certificates.



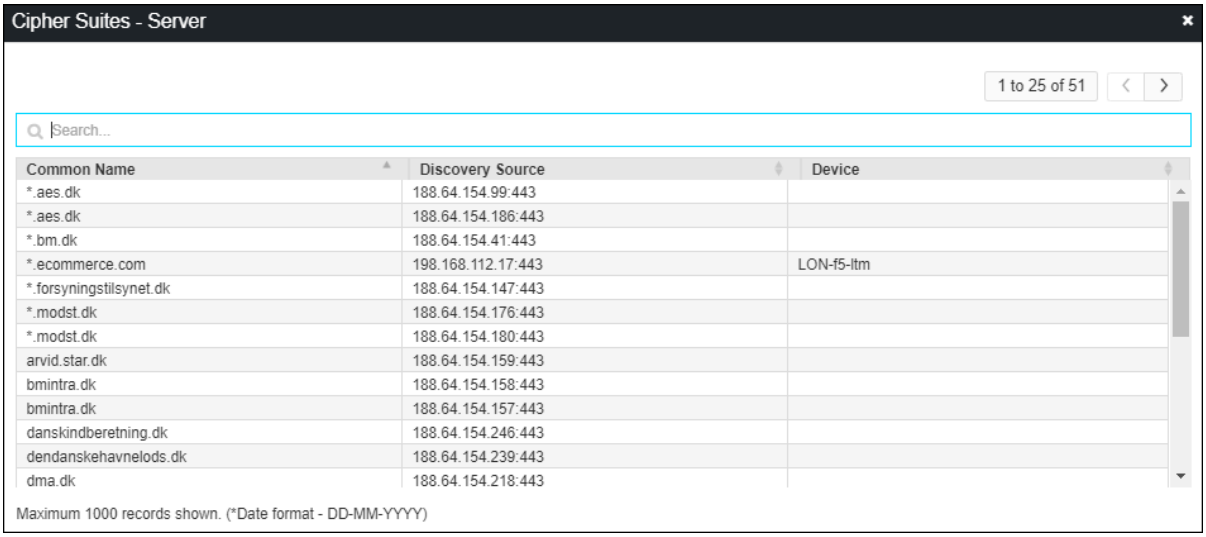
Cipher Suites - Server

This report shows the count of certificates with respect to the cipher suite details and the TLS versions. The cipher suites are shown based on the priority.



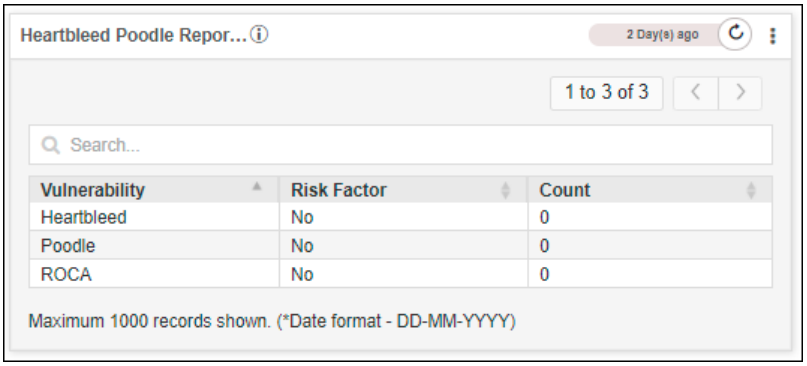
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Clicking on the **Endpoint Count** value in the report displays the respective data of certificates.



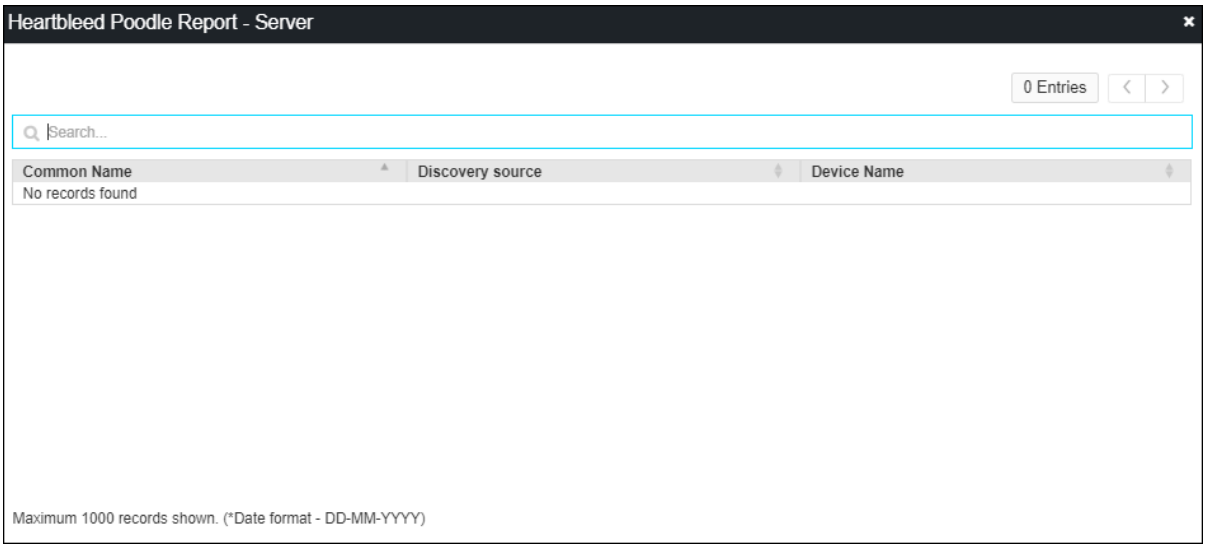
Heartbleed & Poodle Report - Server

This report shows the count of device endpoints are exposed to Heartbleed, Poodle, and ROCA vulnerabilities.



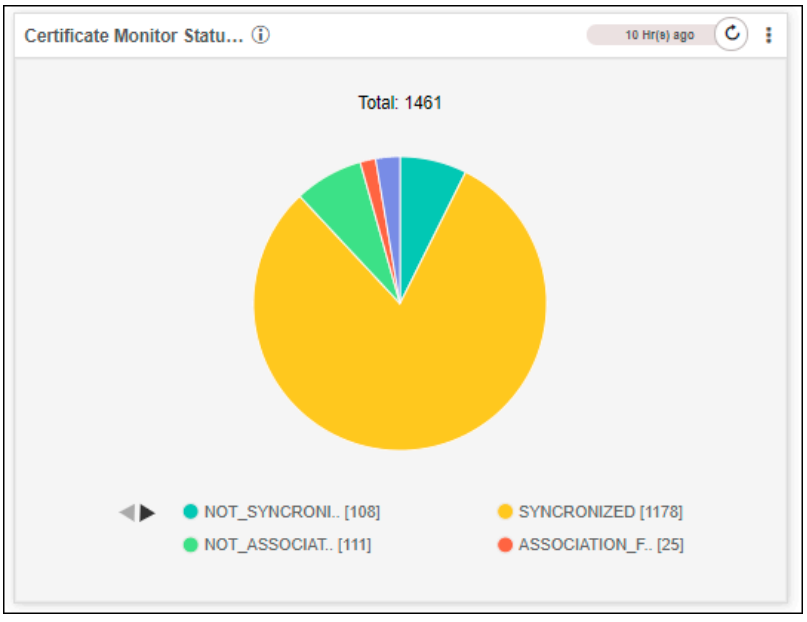
Click on the **Count** value in the report displays the respective data of certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



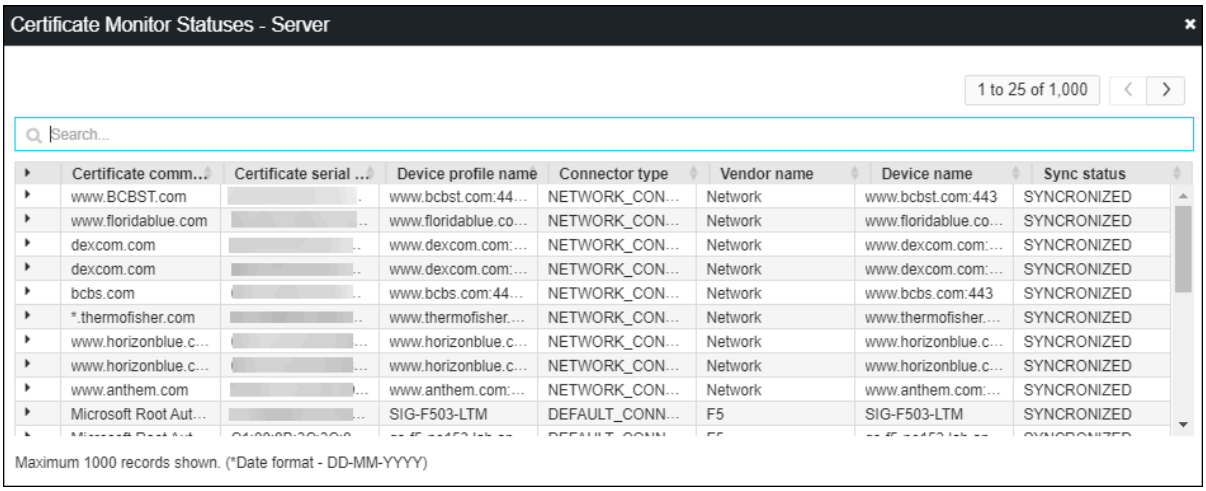
Certificate Monitor Statuses - Server

This report shows the count of domain names for which more certificates are available and only a few are managed/monitored in the Client certificate inventory.



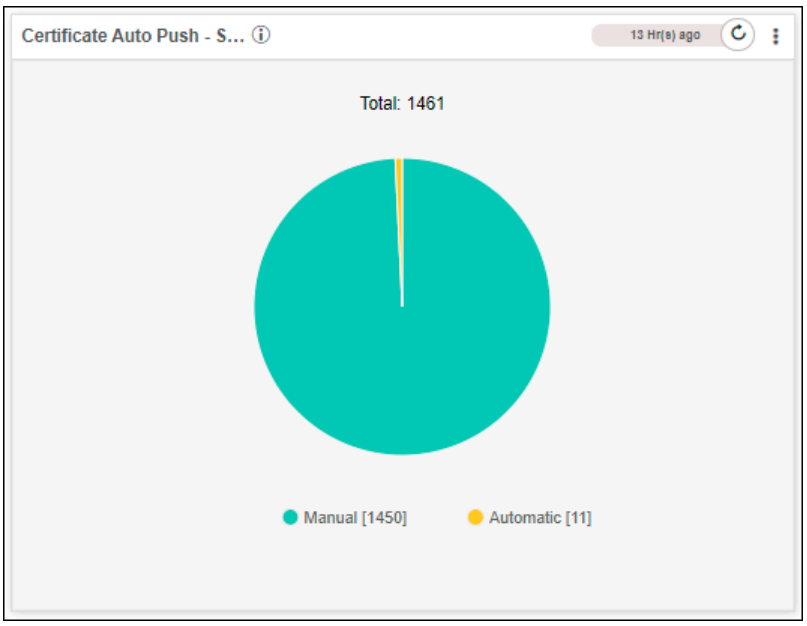
Clicking on any sections of the pie chart displays the respective data of certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Certificate Auto Push - Server

This report shows the count of certificates in the Server inventory which are enabled and not enabled with auto push feature.



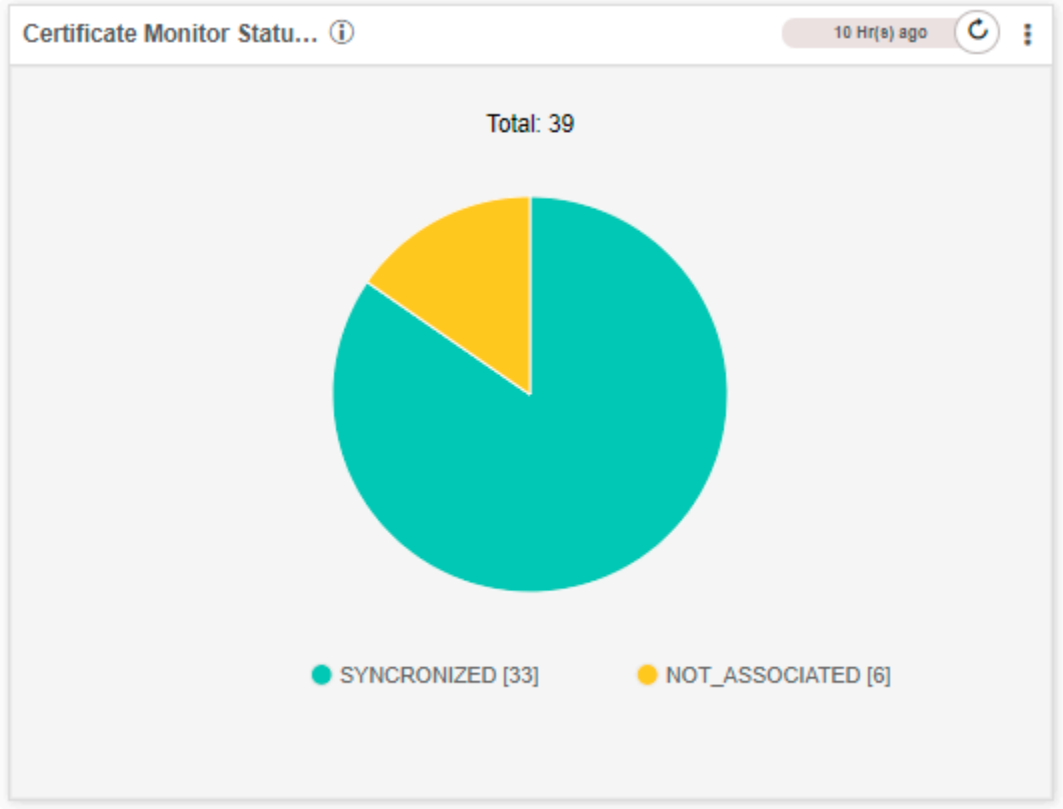
Understanding the Client Endpoint Security Dashboard

For the certificates in the Server inventory which are associated with the endpoints, from the security perspective, the following are the reports available:

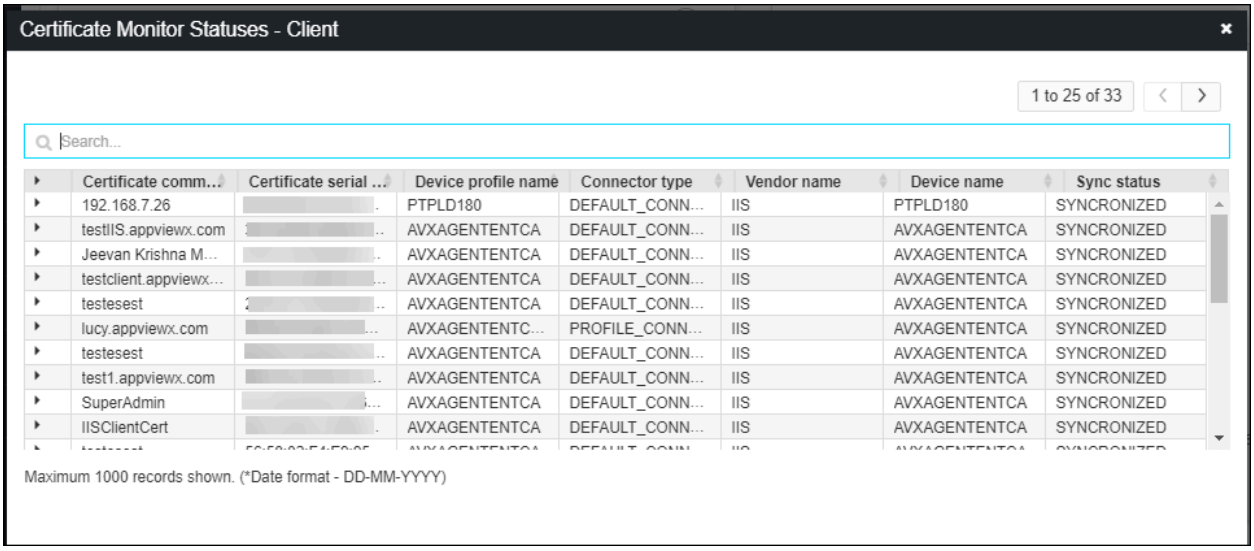
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Monitor Statuses - Client

This report shows the count of endpoints with respect to their certificate monitor statuses available in the client inventory.



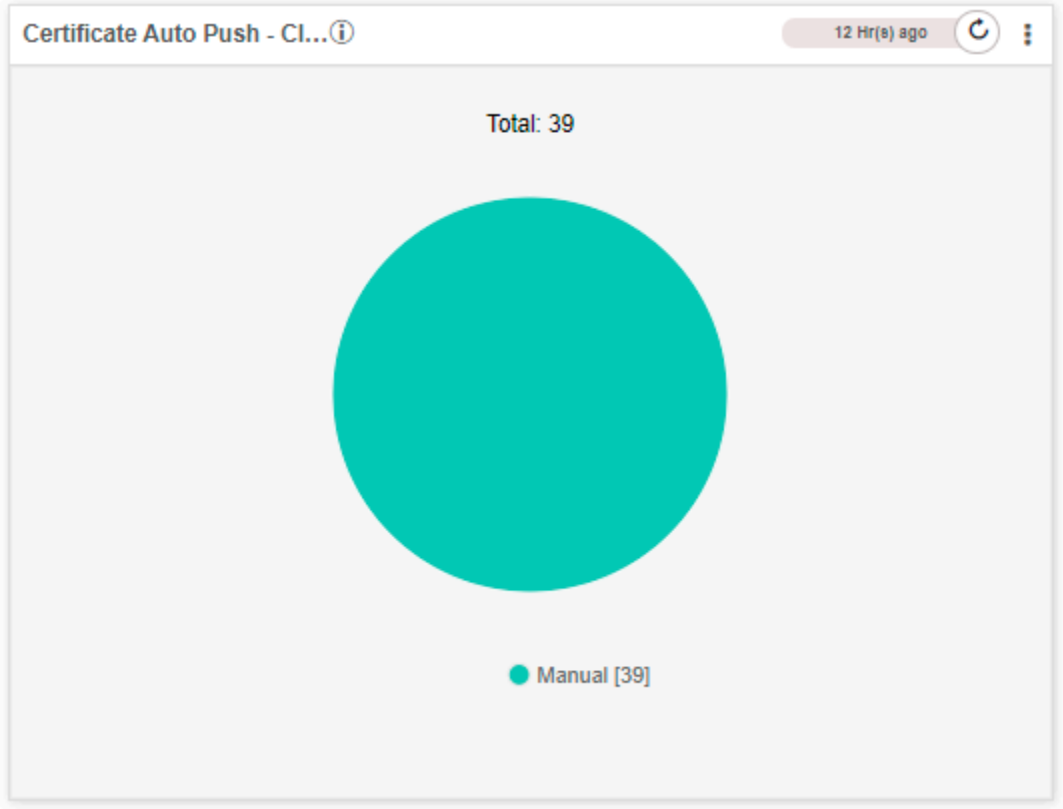
On click of this chart, the respective filtered data of certificates be shown as below:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

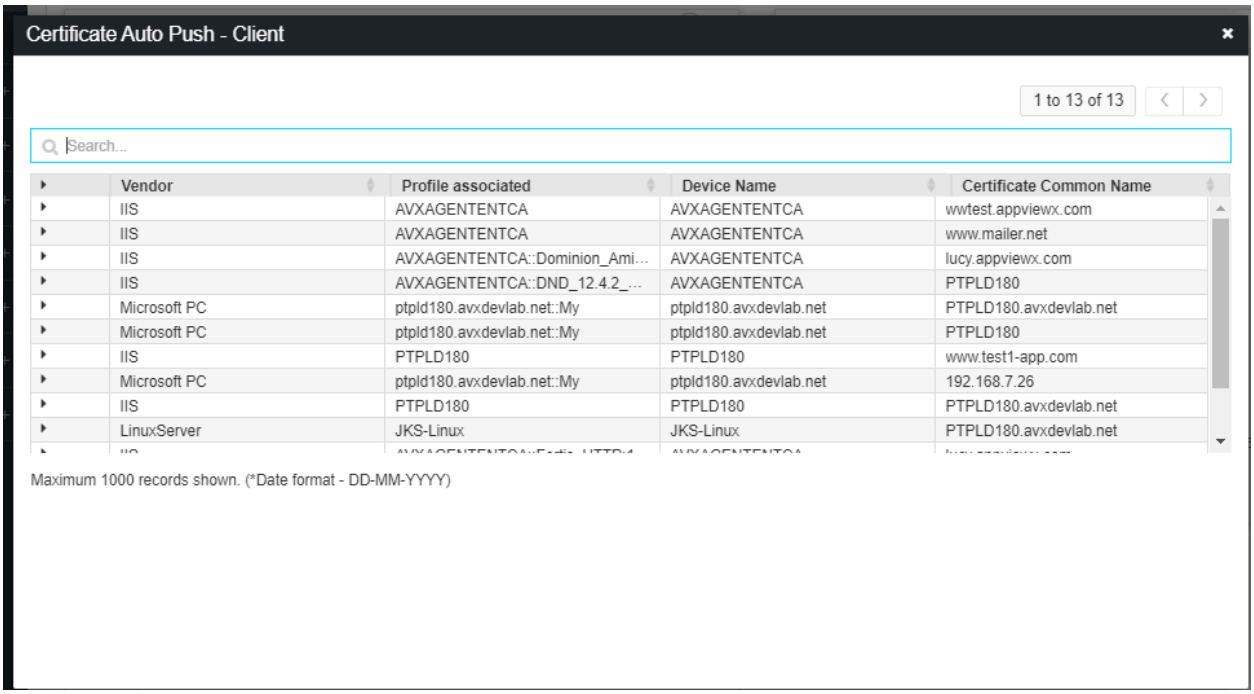
Certificate Auto Push - Client

This report shows the count of certificates in the client inventory which are enabled and not enabled with auto push feature.



On click of this chart, the respective filtered data of certificates be shown as below:

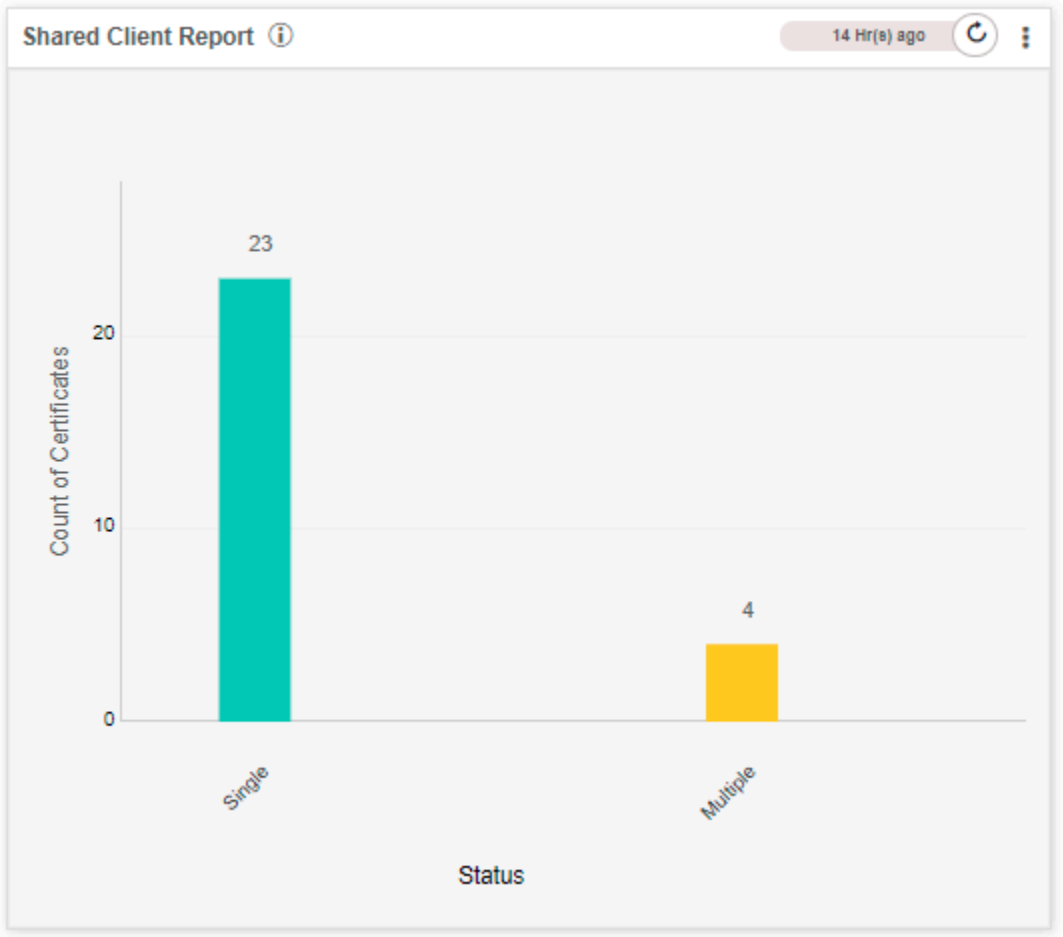
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



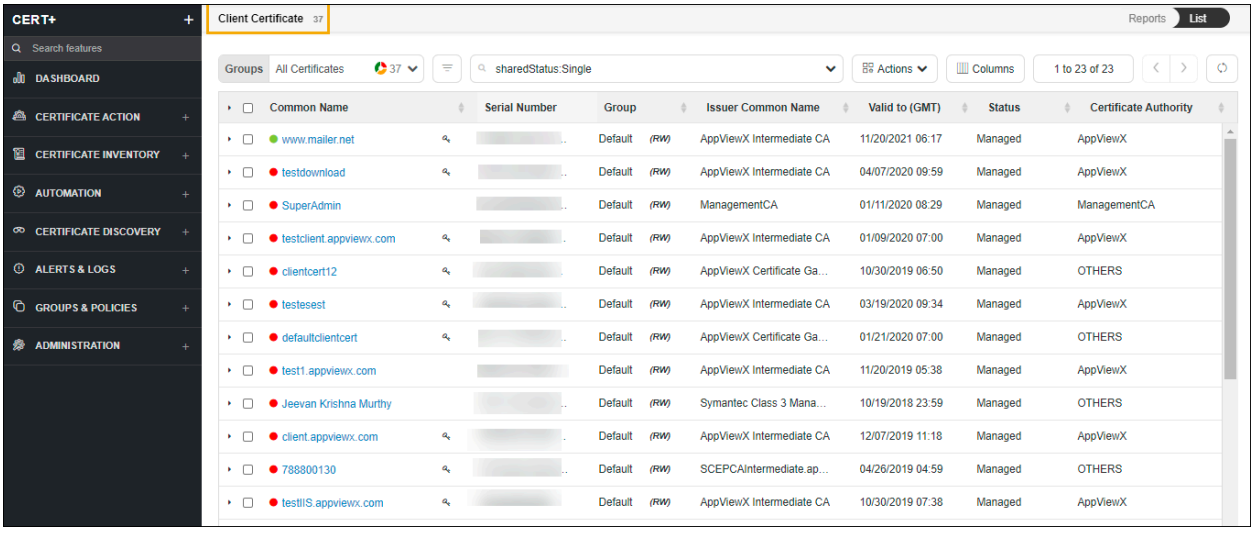
Shared Client Report

This report shows the count of certificates in the client inventory which are shared with a single endpoint or multiple endpoints.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



On click of this chart, the respective filtered data of certificates be shown as below:



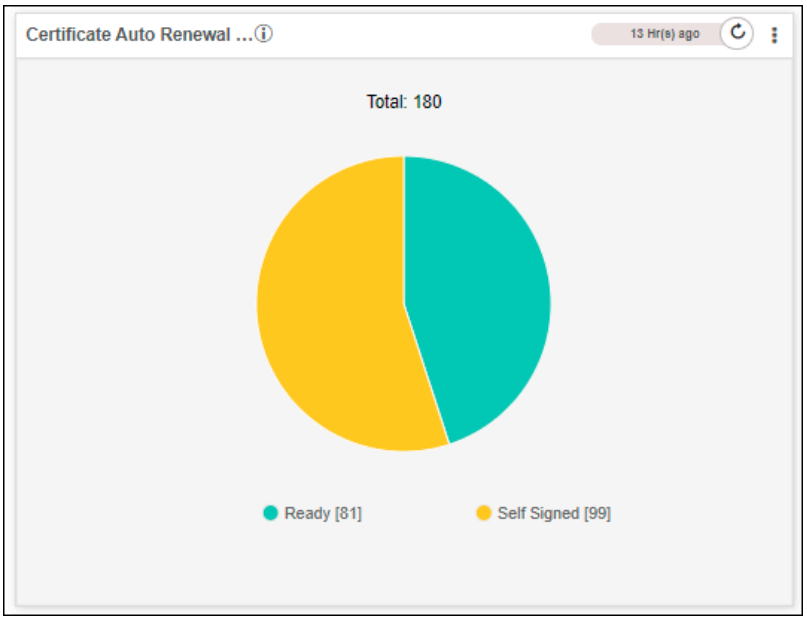
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Understanding the Server Standard Dashboard

For the certificates in the Server inventory, from the standard perspective, the following are the reports available in this dashboard:

Certificate Auto-Renewal Readiness - Server

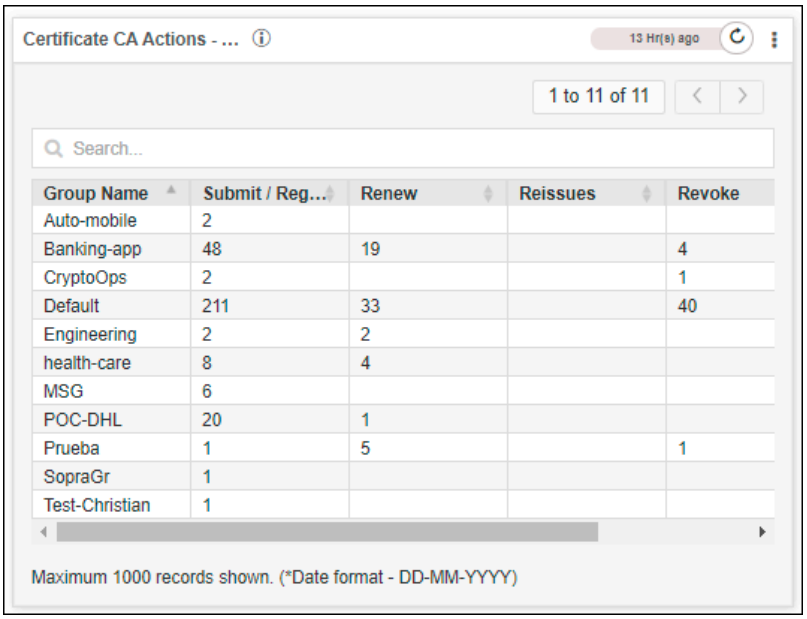
This report shows the count of certificates ready for the auto-renewal process available in the server inventory.



Certificate CA Actions - All Certificate Types

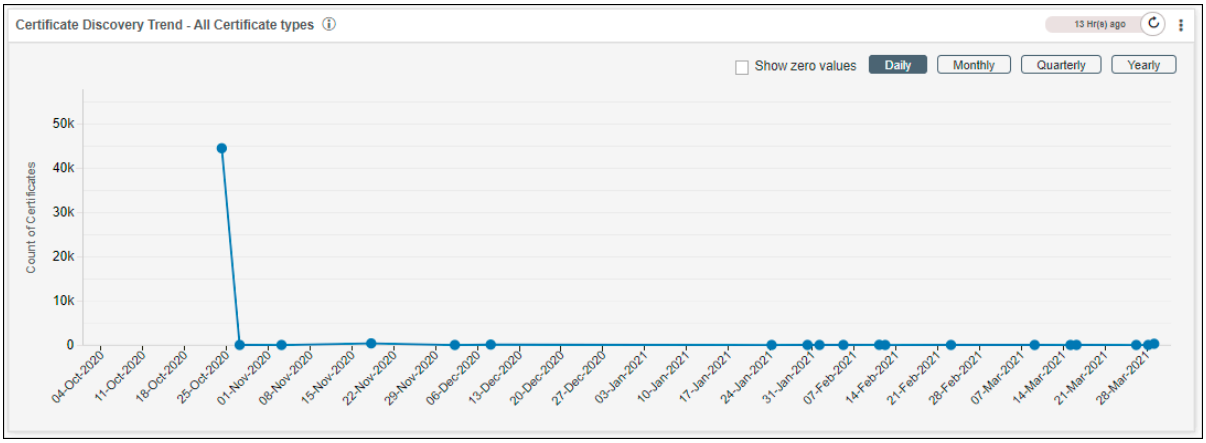
This report shows the count of CA actions performed with respect to the certificate groups available in the server inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Certificate Discovery Trend - All Certificate Types

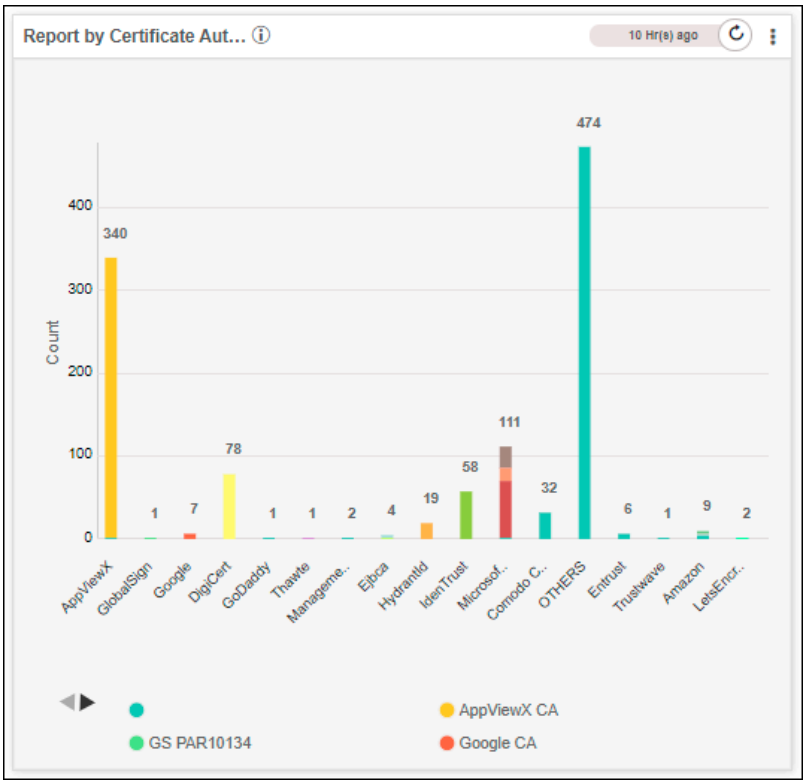
This report shows the trend of the count of certificates discovered into AppViewX in the last year.



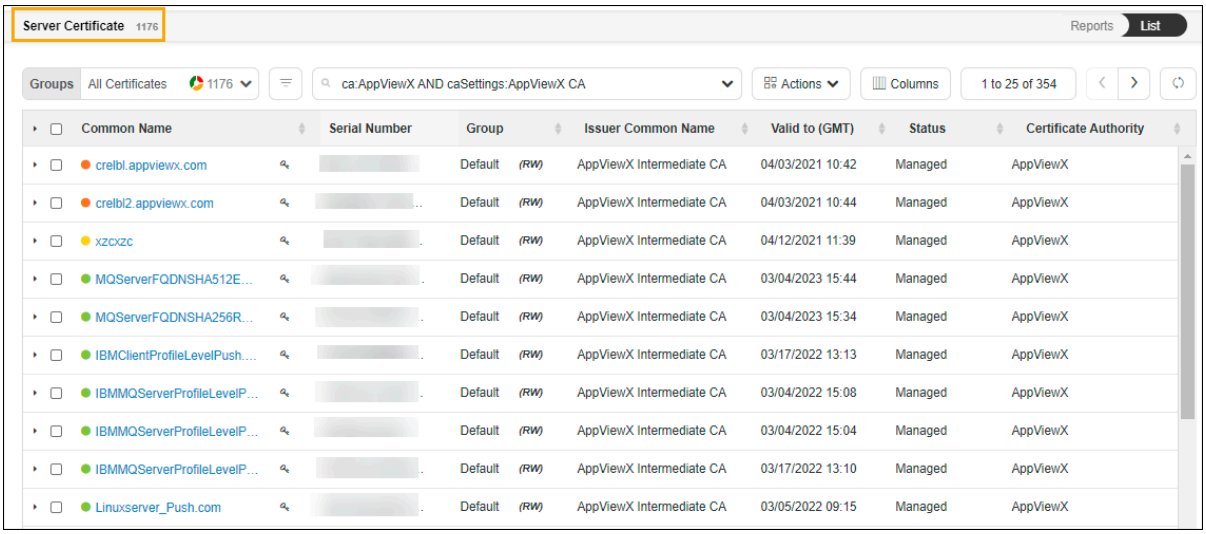
Report by Certificate Authority - Server

This report shows the count of certificates available in the server inventory with respect to the CA accounts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



When you click of the chart, the filtered data of certificates are shown as below:



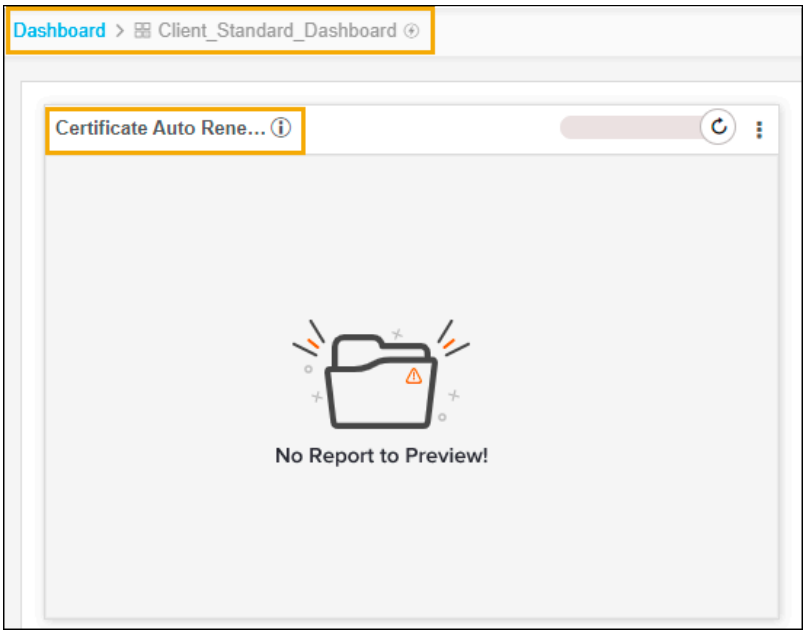
Understanding the Client Standard Dashboard

For the certificates in the Client inventory, from the standard perspective, the following are the reports available in this dashboard:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

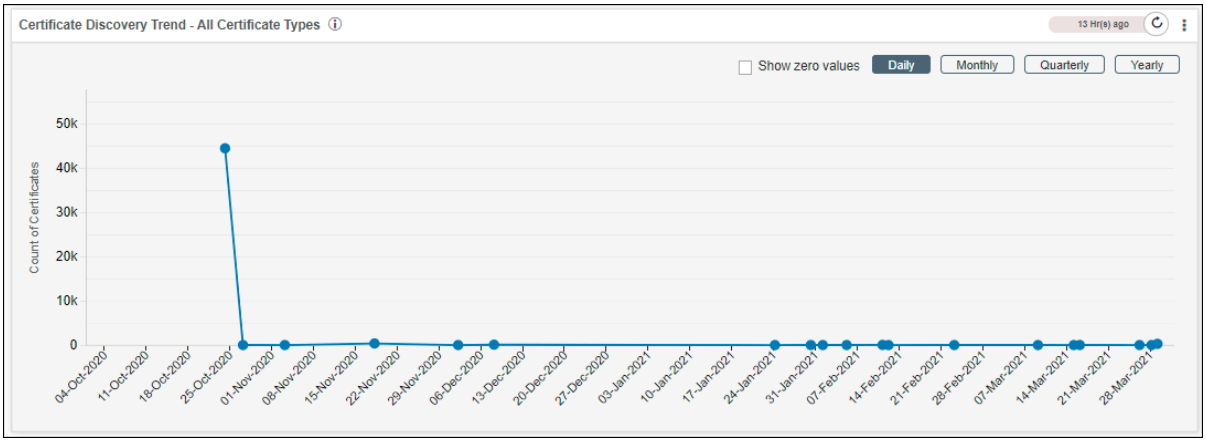
Certificate Auto-Renewal Readiness - Client

This report shows the count of certificates ready for the auto-renewal process available in the Client inventory.



Certificate Discovery Trend - All Certificate Types

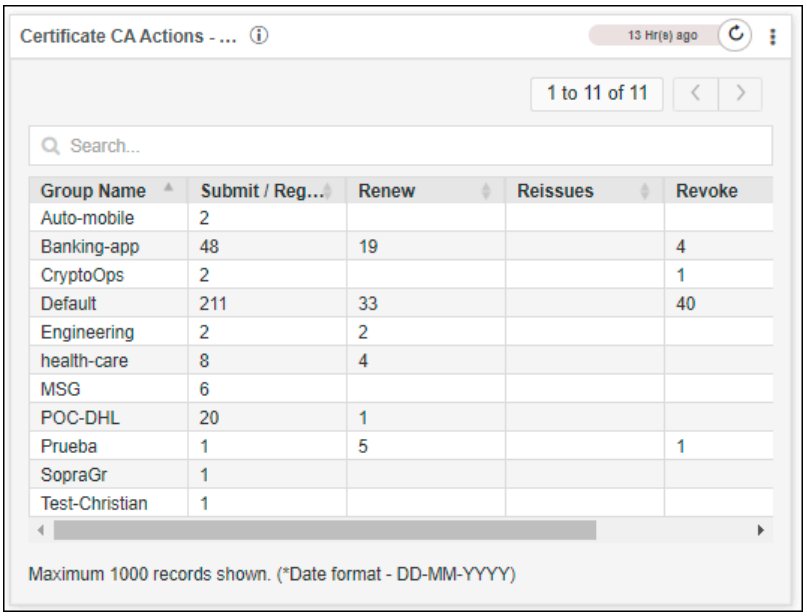
This report shows the trend of the count of certificates discovered in AppViewX in the last year.



Certificate CA Actions - All Certificate Types

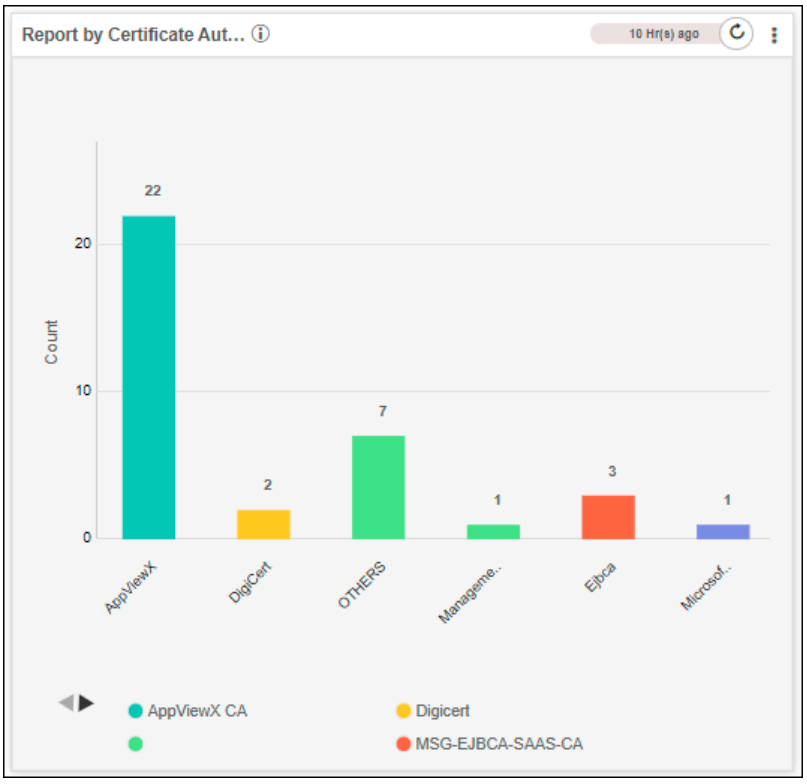
This report shows the count of CA actions performed with respect to the certificate groups available in the Client inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Report by Certificate Authority Accounts - Client

This report shows the count of certificates available in the client inventory with respect to the CA accounts.



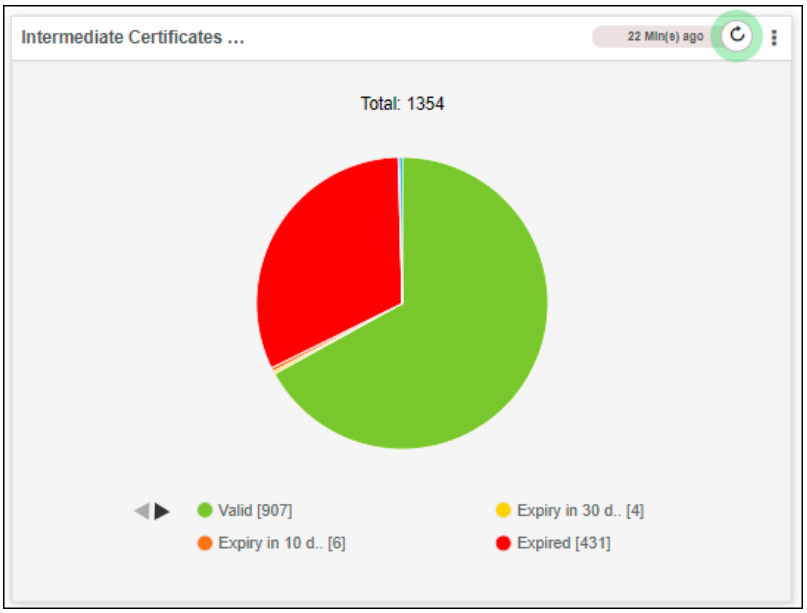
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Understanding the Trust Store Certificates Dashboard

For the certificates in the Root and Intermediate inventories, the following are the reports available in this dashboard:

Intermediate Certificates Expiry Statuses

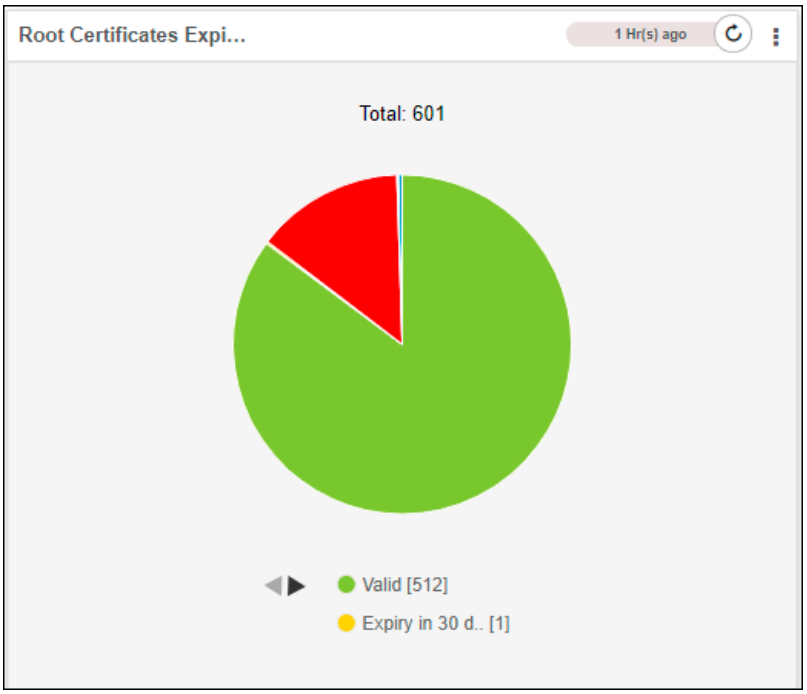
This report shows the count of certificates in the intermediate certificate inventory with respect to the valid and expiry status of the certificates.



Root Certificates Expiry Statuses

This report shows the count of certificates in the root certificate inventory with respect to the valid and expiry status of the certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Report Customization

AppViewX CERT+ allows you to customize your reports based on the organization's needs. Depending on the customization, reports are classified into:

- My Reports
- Store
- Widget

My Reports

Personalized reports can be generated based on a user account. This will be useful when an operator is assigned to do a specific task and has to generate reports on the same. To know more about **My Reports**, refer below.

Creating a New Report

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

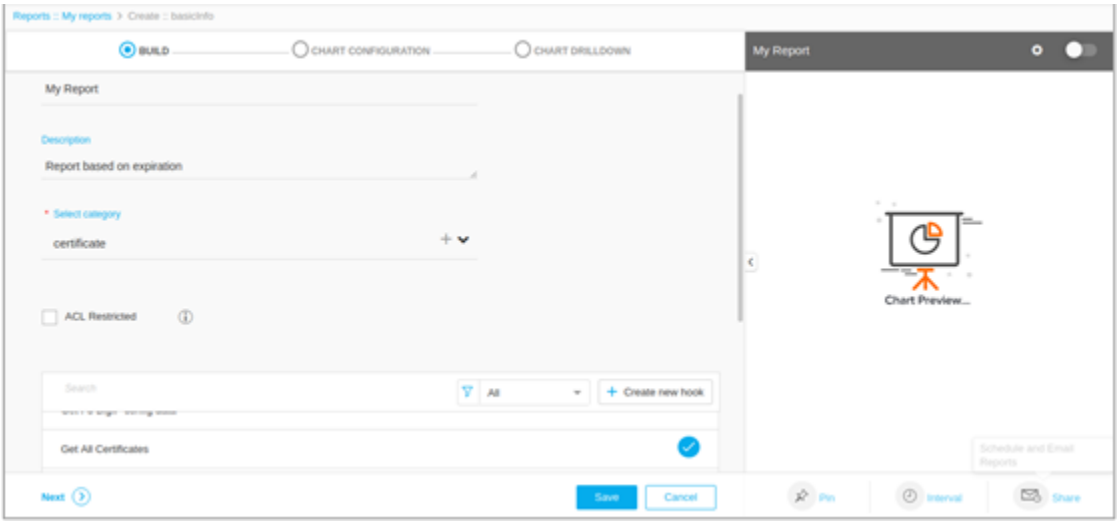
   The left navigation pane appears.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click **Platform > DATA STUDIO > Reports**.

   By default, **My Reports** page will be displayed.

4. Click **Create New Report** on the top-right.
5. On the **Create Report** page, enter the **Report Name**, **Description** and select a **Category** from the list.
6. Enable **ACL Restricted** option if you want the report to be visible based on the user's resource access.
7. Select a hook from the list of available hooks or click **Create New Hook**.
8. Click **Save** to save details.
9. Click **Next** at the bottom-left.



10. On the **Chart Configuration** page, select one of the following chart types:
    - Pie
    - Donut
    - Bar
    - Stacked Bar
    - Grid
    - Line
    - Metric

    - If you have selected **Pie** chart type, choose an option from the **Group By** and **Aggregation** dropdown.

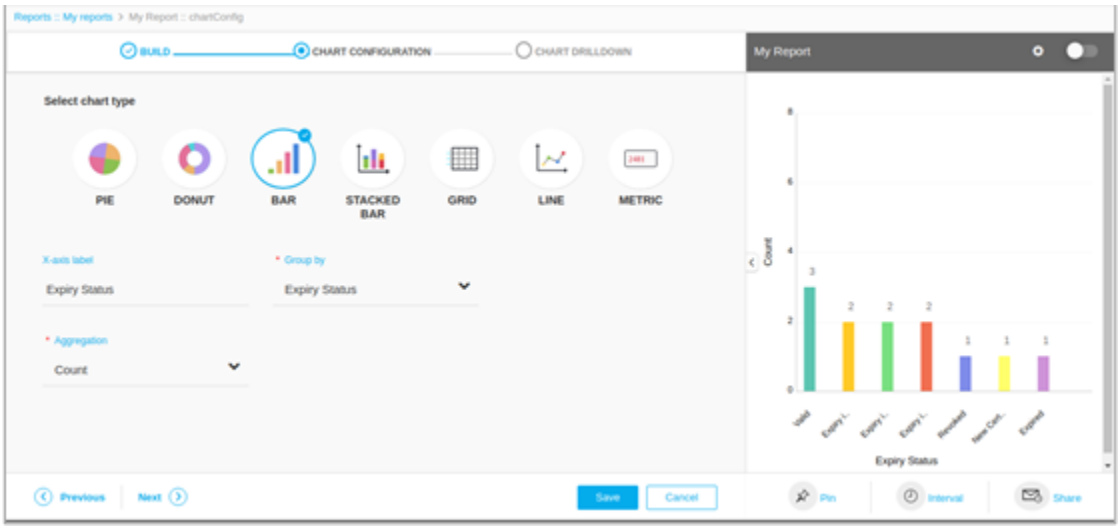
    - If you have selected **Donut** chart type, choose an option from the **Group By** and **Aggregation** dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- If you have selected the **Bar chart** type, fill the **X-axis Label** field and choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Stacked Bar** chart type, fill the **X-axis Label** field and choose an option from the **Group By**, **Aggregation**, and **Stacked By** dropdown.
- If you have selected **Grid** chart type, enable the **Show Column Headers** option if required. Then, under **Columns**, select columns or click the **Select All** option.

> **Note:** For the Select All option, only 10 columns can be selected.

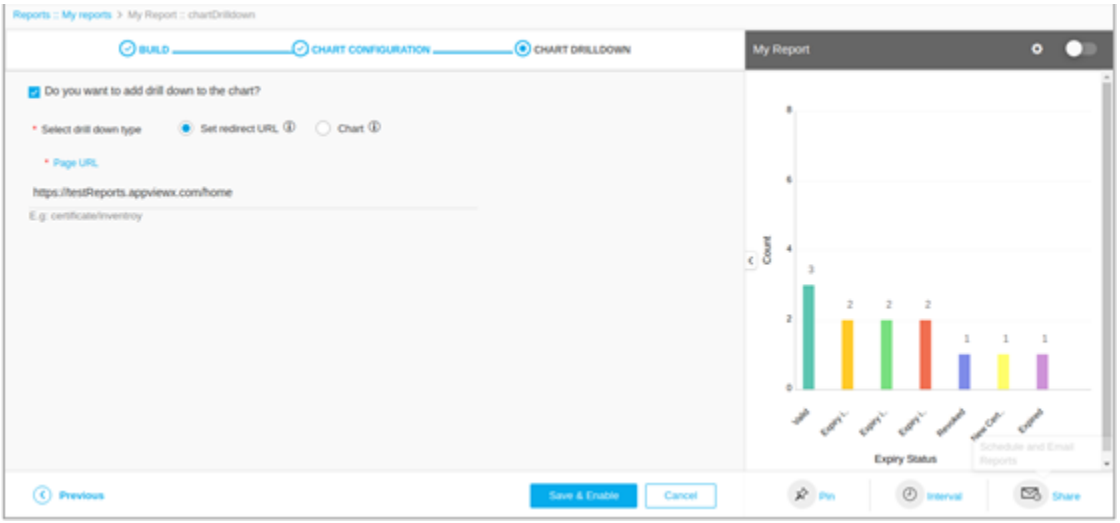
- If you have selected **Grid** chart type, fill the **X-axis Label** field, choose a **Date Format**, and choose an option from the **Group By** and **Aggregation** dropdown.
- If you have selected **Metric** chart type, enter a **Chart Title** and choose an option from the **Aggregation** dropdown. Under **Chart Formatting**, select a chart size, alignment, font color, and icon.



11. Click **Save**.
12. Click **Next** at the bottom-left.
13. On the **Chart Drilldown** page, enable the **Do you want to add drill down to the chart?** option to add drilldown.
14. Click **Save & Enable**.
    The graphical representation of the report will be displayed on the right.
15. To enable the generated report, click the enable icon on the top-right of the report window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

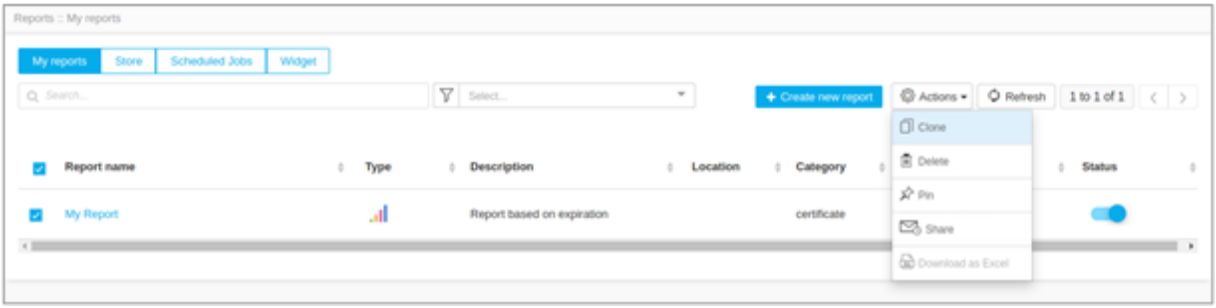
16. To pin the report to a dashboard page, click the **Pin** icon at the bottom right. Select Existing Dashboard or New Dashboard based on where it needs to be pinned.
17. To set the polling interval to collect data, click the **Interval** icon at the bottom right.
18. To share the report, click the **Share** icon at the bottom right.



Cloning a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

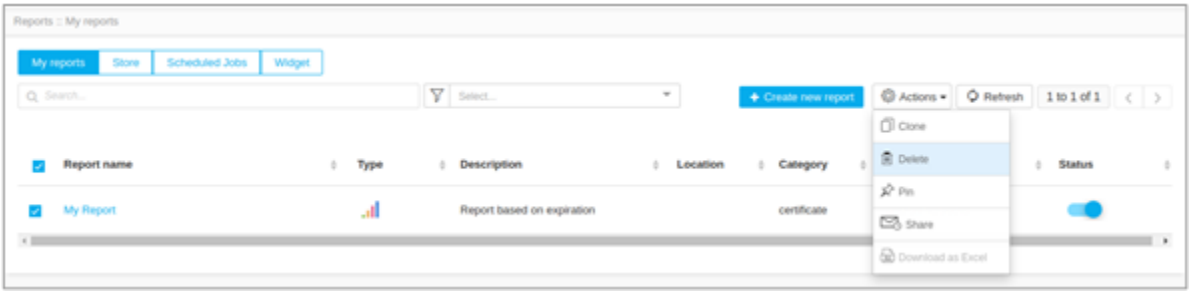
   The cloned reports will be displayed under the **My Reports** tab.



Deleting a Report

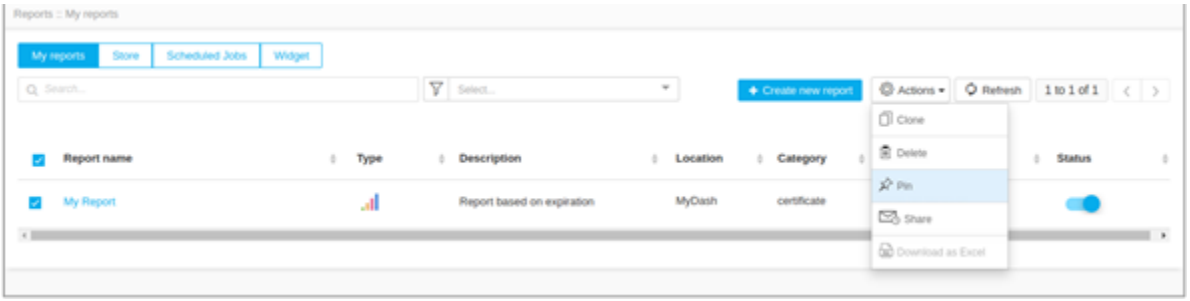
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Delete**.
5. On the **Confirm Delete** popup window, click **Yes**.



Pinning a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.

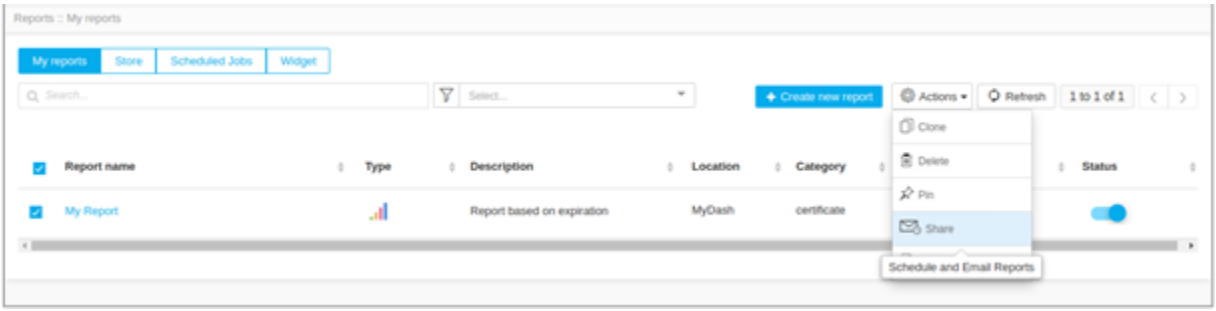


Sharing a Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under **My Reports** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share** to schedule and email reports.
5. On the **Schedule reports** window, fill the **General** section for mail content and **Schedule** section for scheduling emails.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.

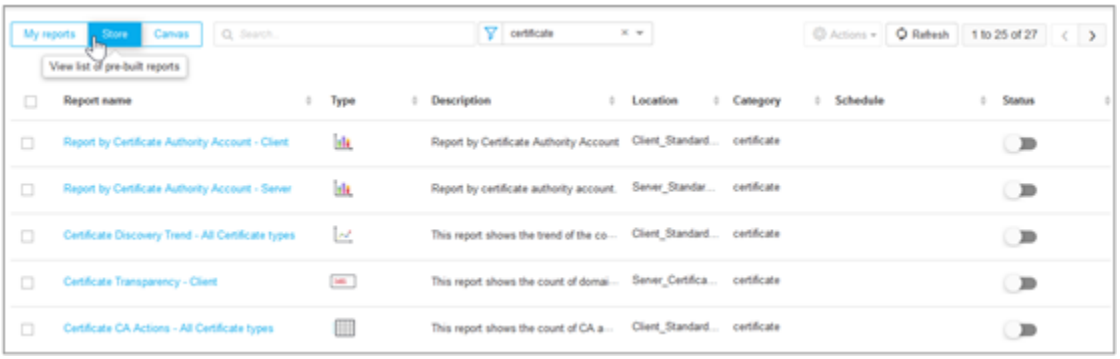


Store

There are a few pre-defined reports available in the store. These reports can be cloned and customized to have personalized reports, but cannot be modified. To know more about **Store**, refer below.

Viewing Pre-built Reports

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.
   The left navigation pane appears.
3. Click **Platform > DATA STUDIO > Reports**.
   By default, the My Reports page will be displayed.
4. Click **Store** on the top-left.
   list of pre-built reports will be displayed.
5. You can search for reports and filter reports by category.

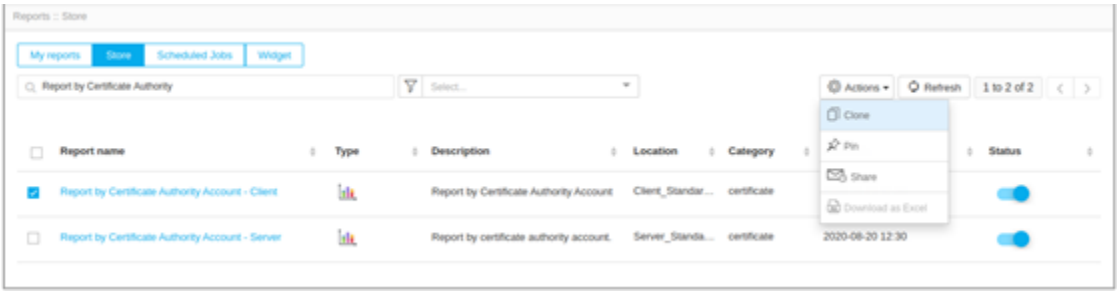


Cloning a Pre-built Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Under the **Store** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

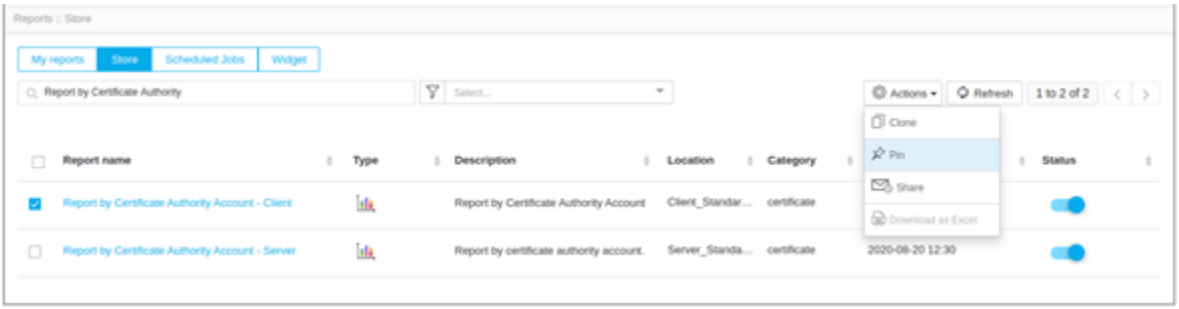


The cloned reports will be displayed under the **Store** tab.

Note: By default, store/pre-built reports are enabled. You cannot disable or delete it.

Pinning a Pre-built Report

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under the **Store** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to the Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.



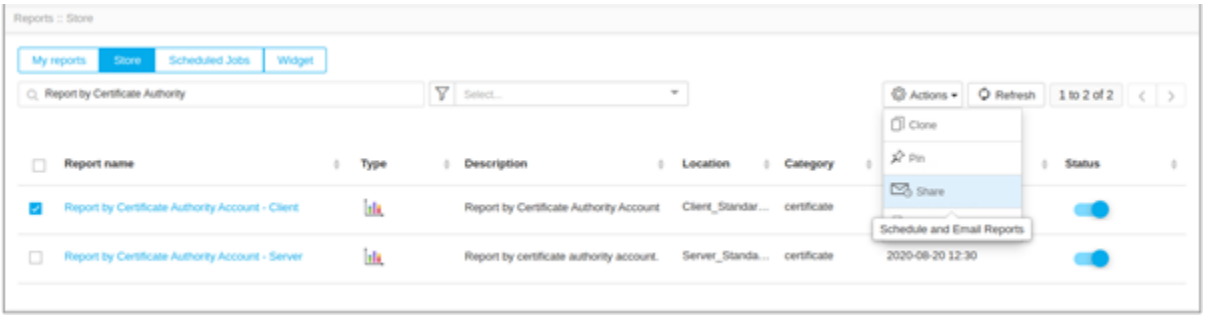
6. Click **Save**.

The pinned reports will be displayed in the dashboard.

Sharing a Pre-built Report

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under the Store tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share**.
5. On the **Schedule reports** window, fill out the **General** section for mail content and **the Schedule** section for scheduling emails.
6. Click **Save**.



Widget

Widget reports are useful when an operator creates their widget based on the business needs. These widgets display the count of a specific operation that is executed and pending in the system. To know more about **Widget**, refer below.

Viewing Custom Reports

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

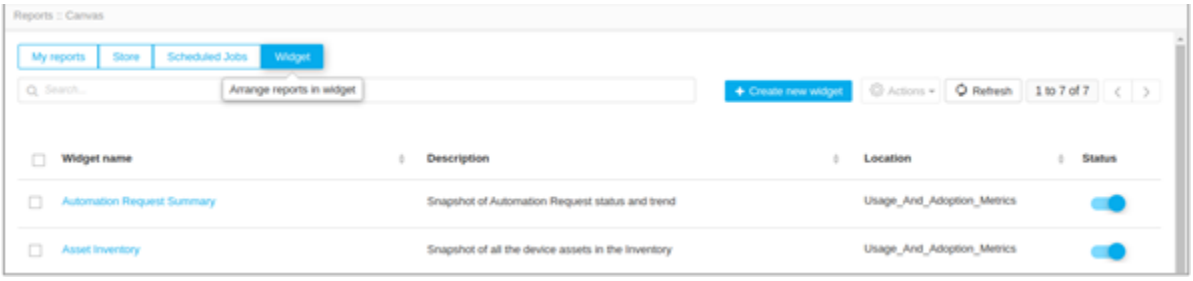
   The left navigation pane appears.
3. Click **Platform > DATA STUDIO > Reports**.

   By default, **the My Reports** page will be displayed.
4. Click **Widget** on the top-left.

   A list of custom reports with the Widget Name, Description, Location, and Status will be displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. You can search for reports and filter reports by category.



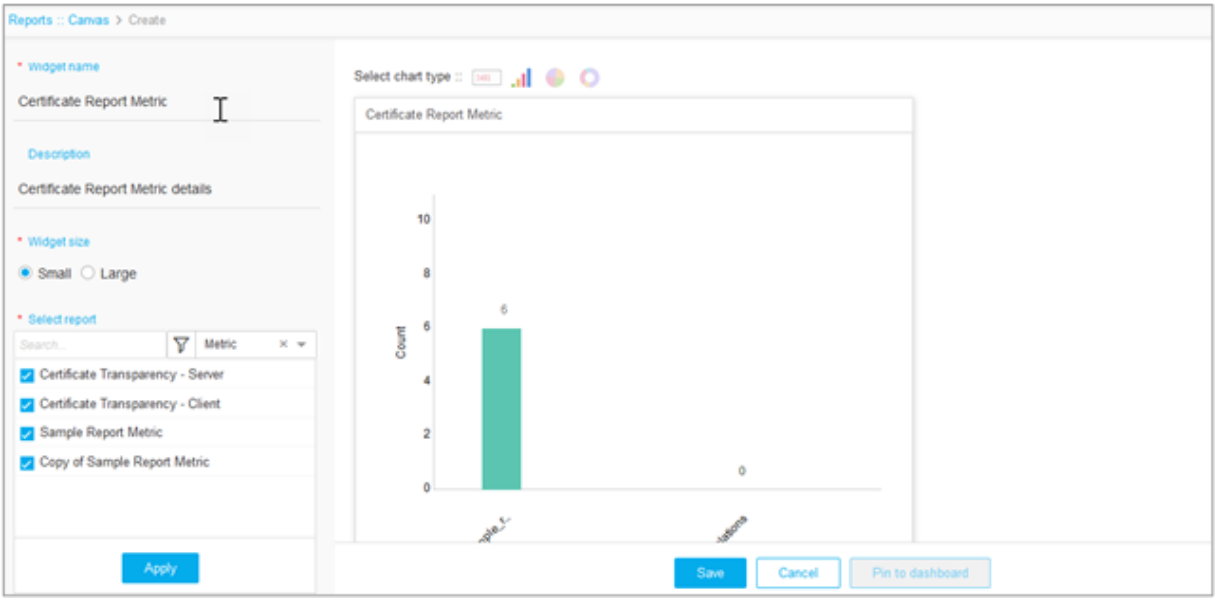
Creating a New Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.

   By default, **the My Reports** page will be displayed.
3. Click **Widget** on the top-left.
4. Click **+ Create New Widget** on the top-right.
5. On the **Create Widget** page, enter a **Widget Name** and **Description**.
6. Select the **Widget Size**: **Small** or **Large**.
7. Under **Select Report**, select a report from the list or search for specific reports.
8. Click **Apply**.
9. Select a **Chart Type**: **Metric**, **Bar**, **Pie** or **Donut**.
10. Click **Save**.
11. Click **Pin to Dashboard** to pin the widget to the existing or new dashboard.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

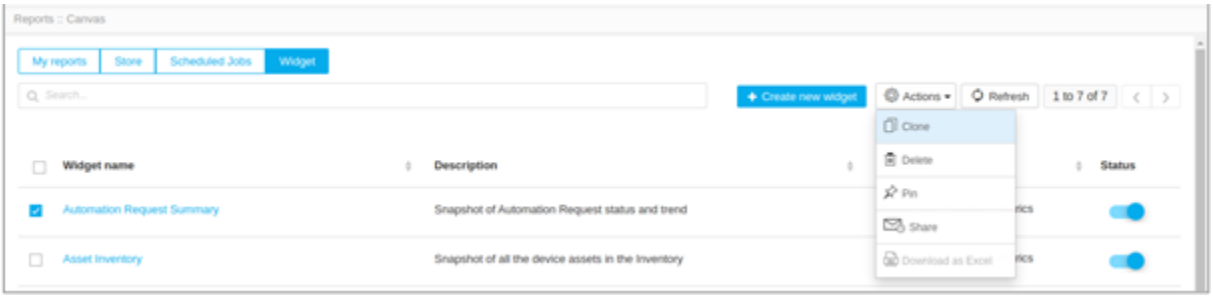
12. To enable the widget status, click the **Status** icon on the top-right.



Cloning a Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Clone**.
5. On the **Clone Report** pop-up window, enter a name.
6. Click **Save**.

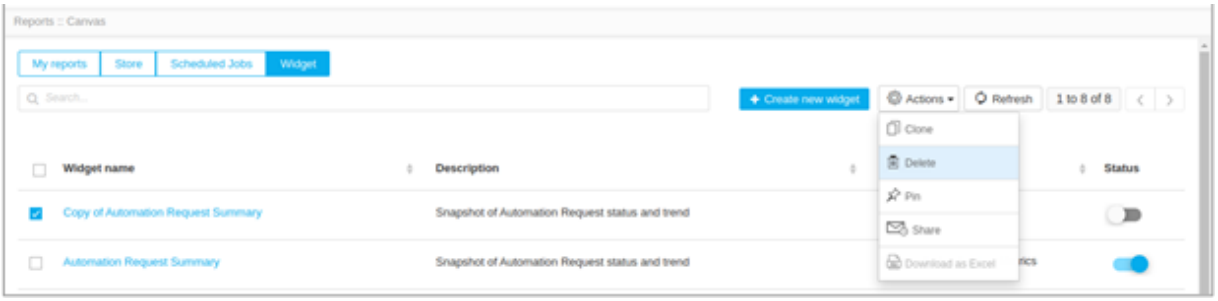
The Cloned reports will be displayed under the **Widget** tab.



Deleting a Widget

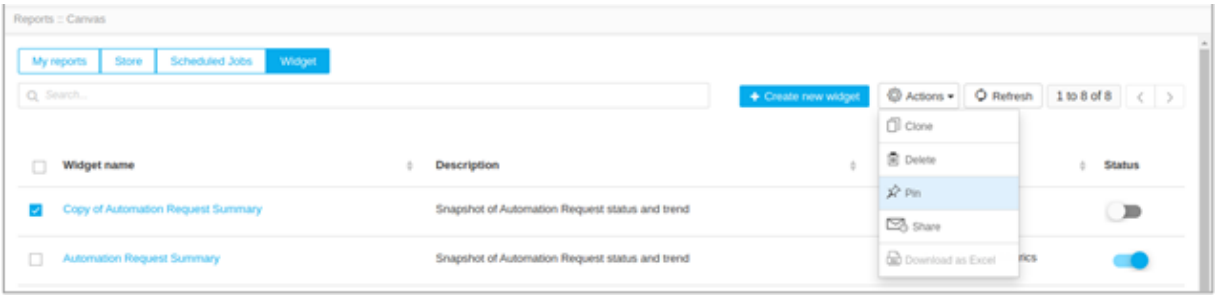
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under the **widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Delete**.
5. On the **Confirm Delete** popup window, click **Yes**.



Pinning a Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Pin**.
5. On the **Pin report(s) to Dashboard** popup window, select Existing Dashboard or New Dashboard based on where it has to be pinned.

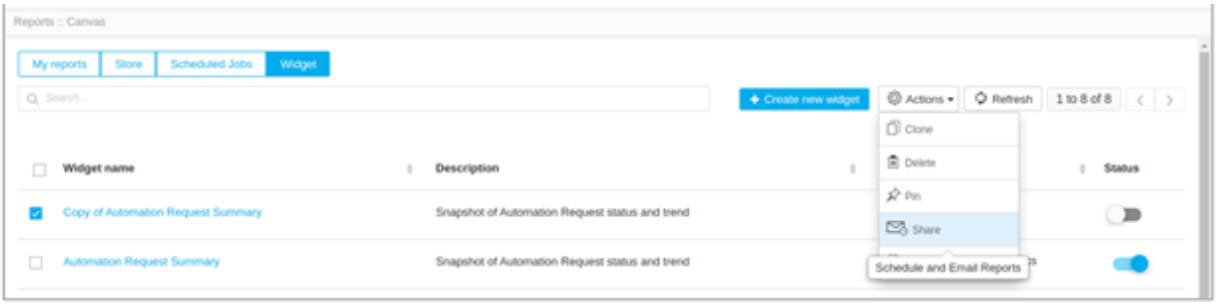


Sharing a Widget

1. Log in to the **AppViewX** application with valid credentials.
2. Click **Menu > Platform > DATA STUDIO > Reports**.
3. Under the **Widget** tab, enable the checkbox to select a report.
4. Click **Actions** dropdown on the top-right and select **Share**.
5. On the **Schedule reports** window, fill out the **General** section for mail content and **the Schedule** section for scheduling emails.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save.**



Security Posture Determination and Interpretation

Application security score reports, TLS, and Cipher suite reports allow you to identify the security level of service. To reduce security risks, change the application configuration to restrict the cipher suites and the TLS versions that are marked as LOW. Also for certain applications, OS upgrades will be applied to align with the security standard.

You can generate security reports through,

TLS Report

TLS report fetches data from SSL sessions and generates the report. It makes it easy for customers to check the protocol version of their servers based on this data. This report will generate data to identify vulnerable protocol versions. For example, in your infrastructure, there may be endpoints that still support TLSv1.0 and TLSv1.1 versions.

The **TLS version - Server** report is available on the **Server Endpoint Security** dashboard.

Cipher Suites Reports

Some ciphers use SHA1 that is still supported by servers. Cipher Report will discover servers that support these ciphers and provide data as per security standards. This report will generate data to identify vulnerable ciphers.

The **Cipher Suites - Server** report is available on the **Server Endpoint Security** dashboard.

Generating Application Score Reports

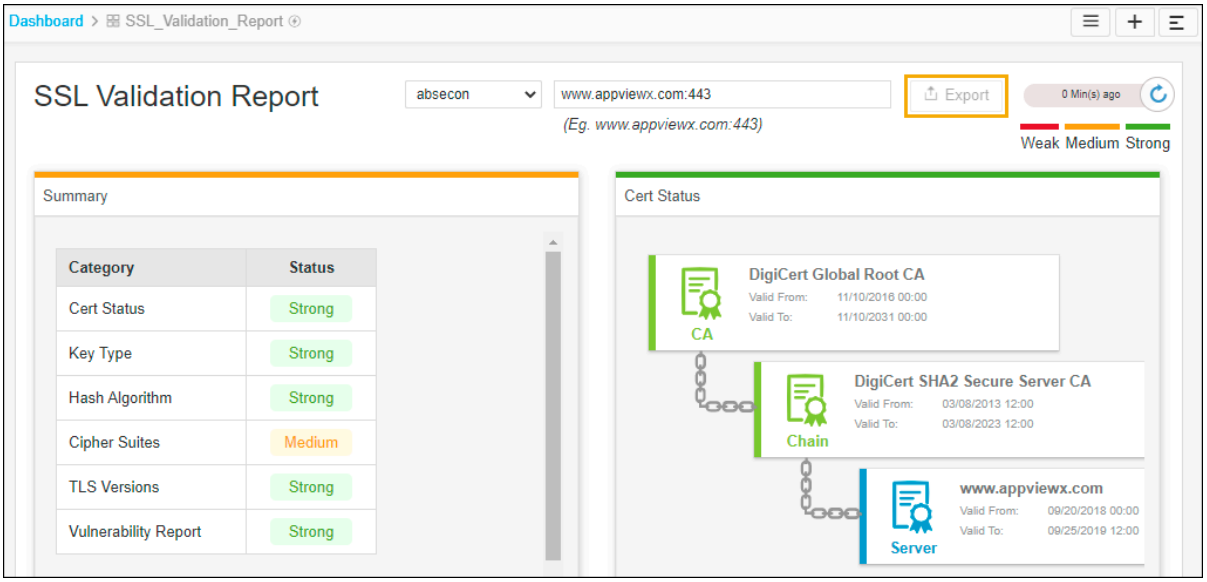
The application score report provides security scores of certificate parameters based on industry standards. You can get the score based on parameters such as Cert Status, Key Type, Hash Algorithm,

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CAA Record, TLS Version, and Vulnerability. Also, you can search for domains and check the security score. For example, you can check if the certificate name is valid through this report.

To generate application score reports:

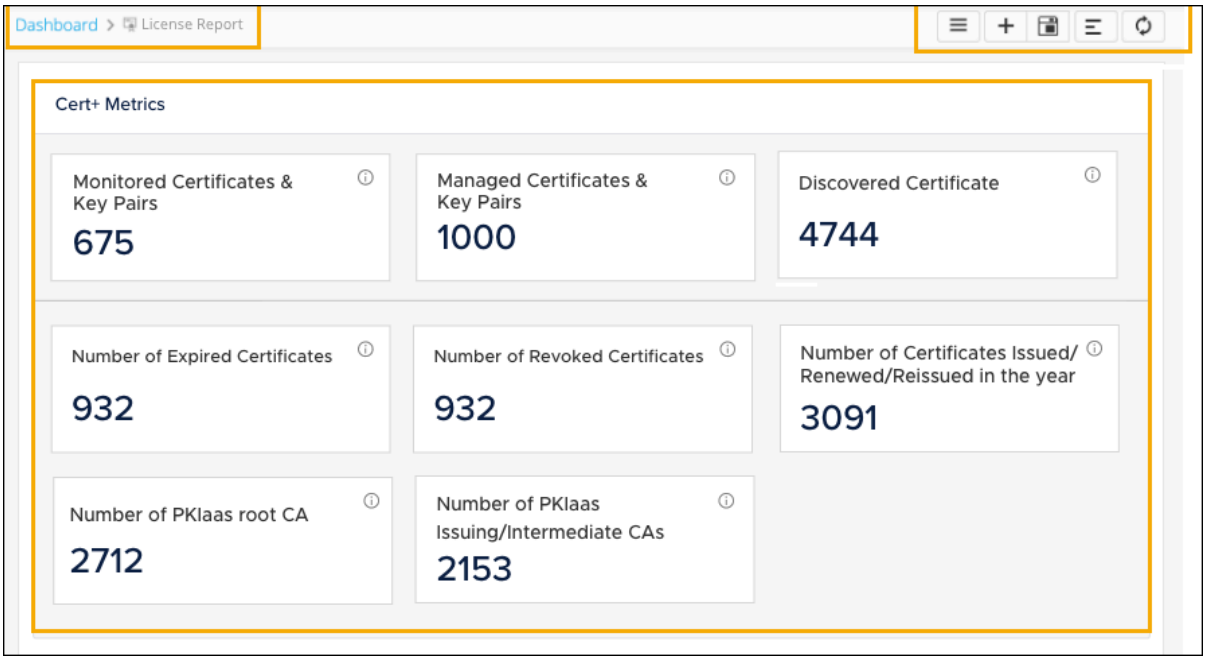
1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The list of dashboards is displayed.
2. On the dashboard page, click **SSL Validation Report**.
3. Select a data center from the first dropdown.
4. In the search bar, enter a domain name (www.appviewx.com:443) and press **Enter**.
   The report is generated with the summary and all required parameters.
5. To export this report as a PDF, click **Export**.



License Report

The License Report dashboard displays the usage count of all the key metrics related to the license. It can be accessed from the Dashboard page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Options available on the License Report dashboard

Options	Descriptions
	Go to Dashboard page where all the Dashboards are listed.
	Create a dashboard/widget.
	Save the widget changes.
	Align the widgets within the dashboard.
	Refresh a dashboard.

Discovery

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Searching for Dashboard, Object, or Widget

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The list of dashboards is displayed.
2. Enter the search keyword in the search field, and then press **Enter**.
   The dashboards, objects, or widgets that match with the specified keyword are displayed.

Deleting a Dashboard

The default dashboard cannot be deleted from the AppViewX platform. Only the customized dashboard can be deleted and deleting the dashboard includes the deletion of all the widgets on the dashboard also.

To delete a dashboard,

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The list of dashboards is displayed.
2. Select the checkbox corresponding to the dashboard you want to delete.
3. From the command bar, click .
4. In the **Confirmation** dialog box, click **Yes**.

> **Important:** Deleting a dashboard will delete all the widgets displayed for the dashboard.

Insights

- Accessing Insights
- Insights Summary
- Insights Operations
- Insights Risk and Crypto
- Insights Entrust Migration
- Google 90 Day Dashboard

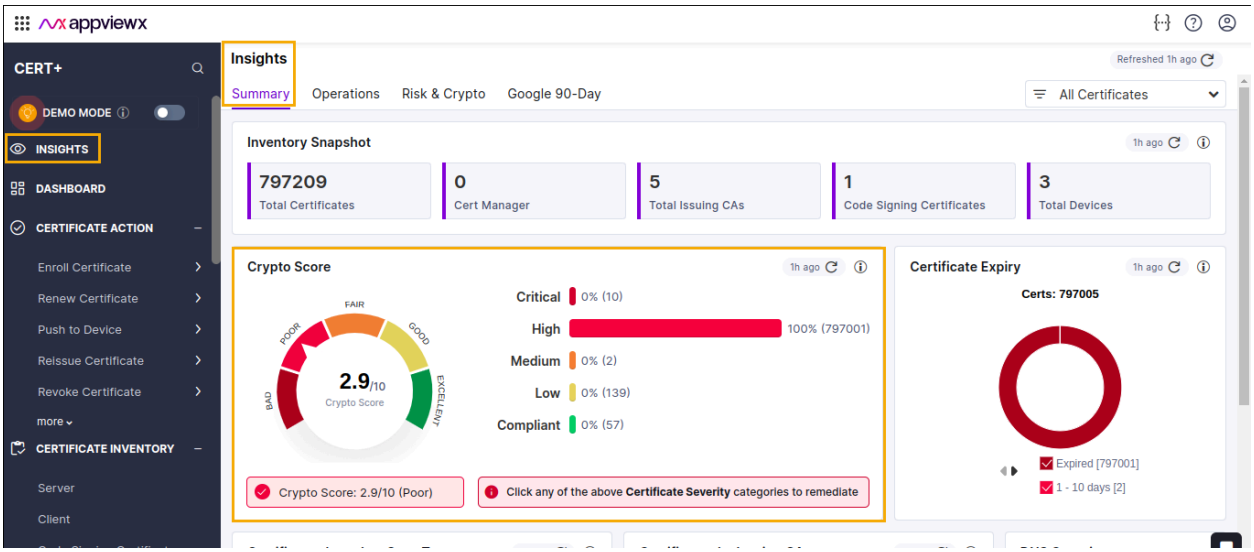
Accessing Insights

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The INSIGHTS menu provides comprehensive information and analytics regarding the overall certificates summary, operations, Risk & Crypto, and Google 90-Day delivered through the CERT+ infrastructure. The INSIGHTS menu populates with relevant data, once the certificates have been successfully onboarded and discovered. Each reports within the INSIGHTS menu refreshes every four hours at regular intervals.

To access the INSIGHTS page, navigate to **Menu** > **CERT** > **INSIGHTS**. These insights are organized into the following tabs:

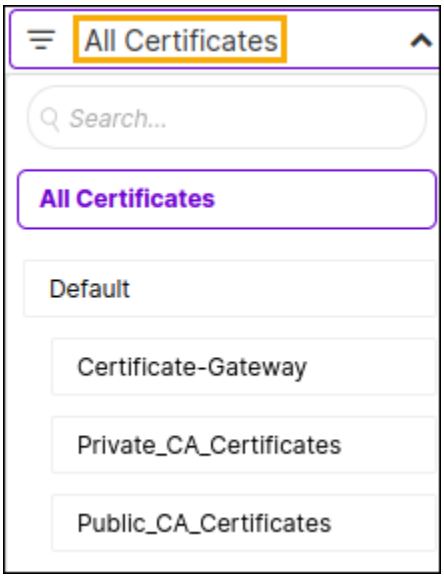
- Summary
- Operations
- Risk & Crypto
- Google 90-Day.



Group Level Filter

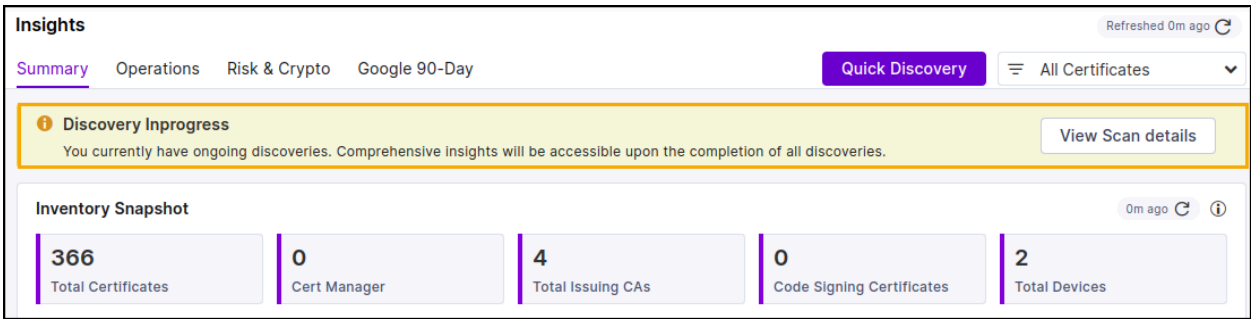
The group-level filter is available in the Insights section of the Summary, Operations, and Risk & Crypto pages. It allows you to filter the reports based on the groups.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Discovery In-progress Notification

On the Insights page, whenever the certificate on-demand discovery operation is in progress, a popup message will notify you on all Insights pages: **You currently have ongoing discoveries. Comprehensive insights will be accessible upon the completion of all discoveries**.



Note: All reports in the respective tab will be refreshed every one minute while the certificatediscovery is in progress, as long as users remain on the Insights page and the certificate count is less than 1 lakh

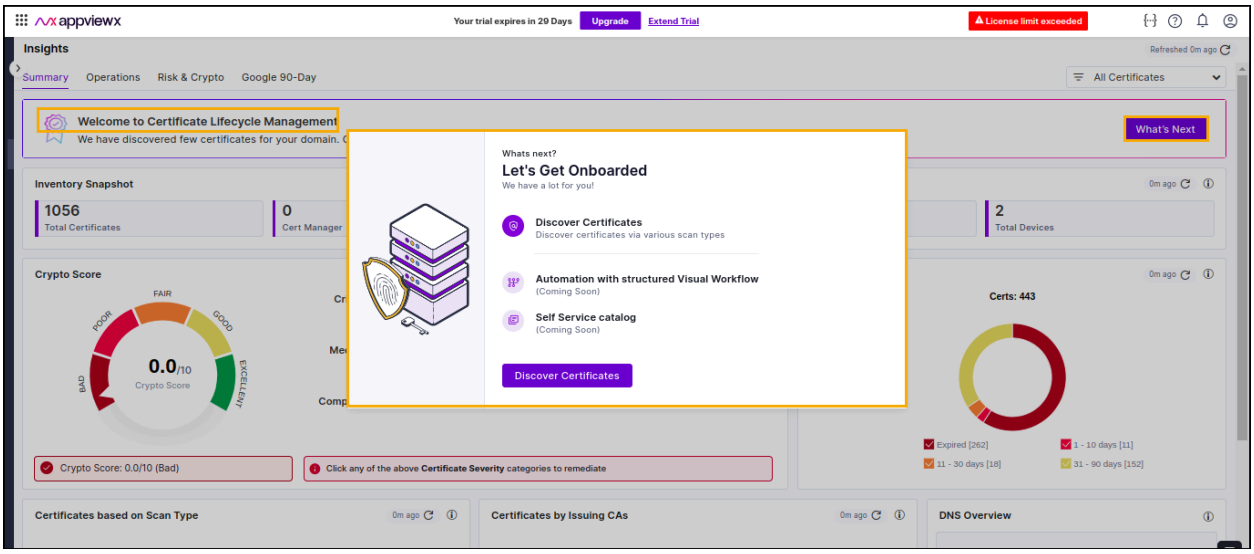
Clicking the "**View Scan Details**" button redirects you to the Discovery Status: On-demand page.

CT Logs Scan

When you onboard a new tenant, CT logs will be triggered for the user's domain. The snack-bar will display a Welcome message such as "**Welcome to Certificate Lifecycle Management**" for different

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

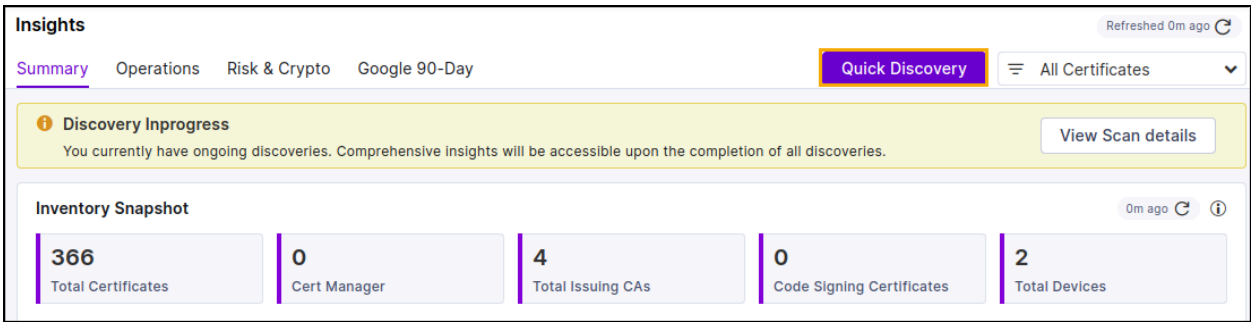
scenarios including Successful, In-progress, and Success or failure with zero certificates. This will appear in the Insights section of the Summary, Operations, Risk & Crypto pages, and Google 90-Day pages.



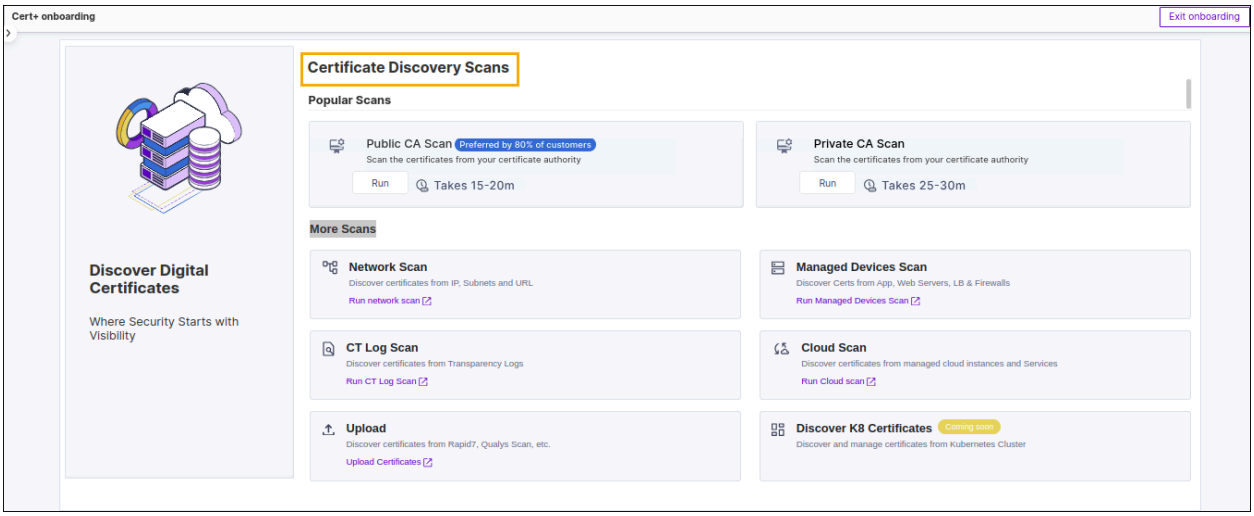
Quick Discovery

The "Quick Discovery" button allows you to access certificate discovery scans, listing all types as follows:

- Popular Scans:
  - Public CA Scan
  - Private CA Scan.
- More Scans:
  - Network Scan
  - Managed Devices Scan
  - CT Log Scan
  - Cloud Scan
  - Upload Scan
  - Discover K8 Certificates.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

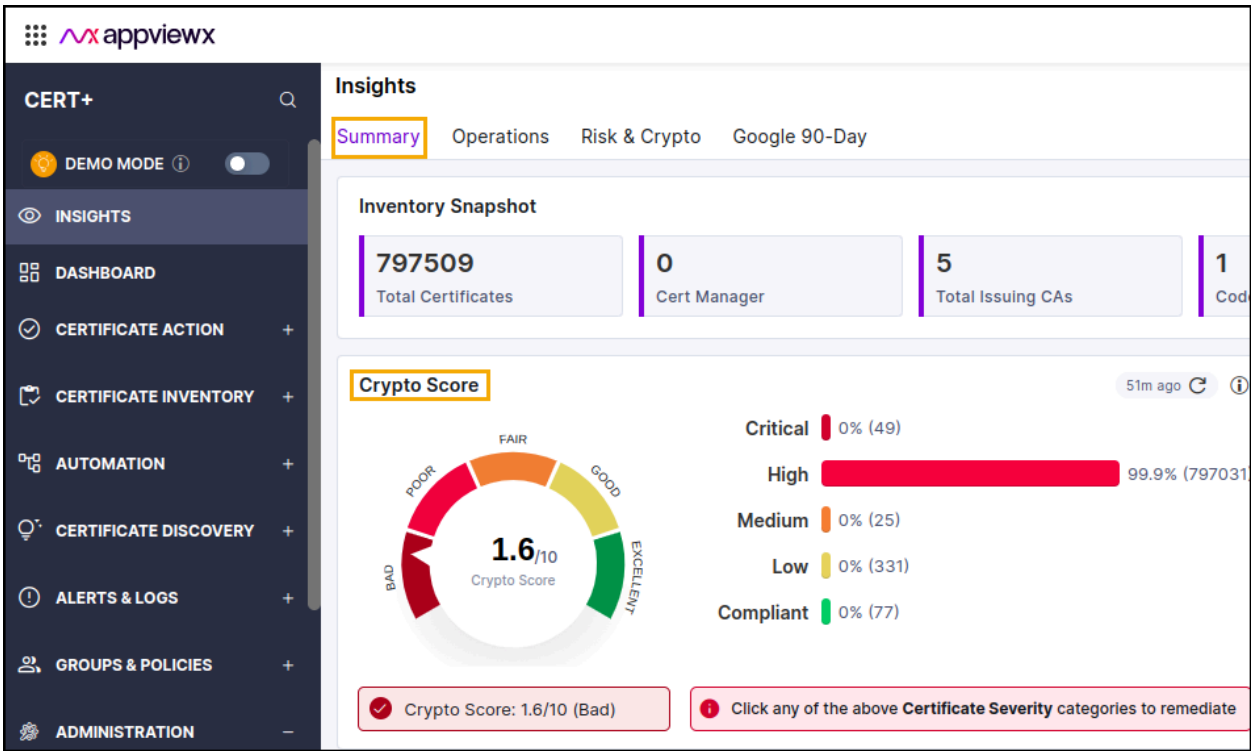


Insights Summary

The Insights Summary report presents a concise overview of the Inventory Snapshot, Crypto Score, Certificates Expiry, Certificates based on Scan Type, and issuing CAs managed within AppViewX. Click on any widget to access detailed information specific to that particular summary on the respective widgets popup. Within the popup window, you can view all the entries, export the content in the desired format if needed, and redirect to inventory. The Widgets within the Insights Summary report are:

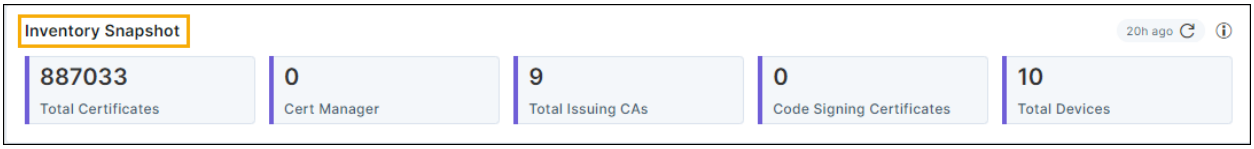
- **Inventory Snapshot**
- **Crypto Score**
- **Certificates Expiry**
- **Certificates based on Scan Type**
- **Certificates by issuing CAs**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Inventory Snapshot

The Inventory Snapshot widget displays the count of certificates, Cert manager, CAs, and Devices that are managed or monitored within AppViewX. The metrics within Inventory Snapshot widget are:

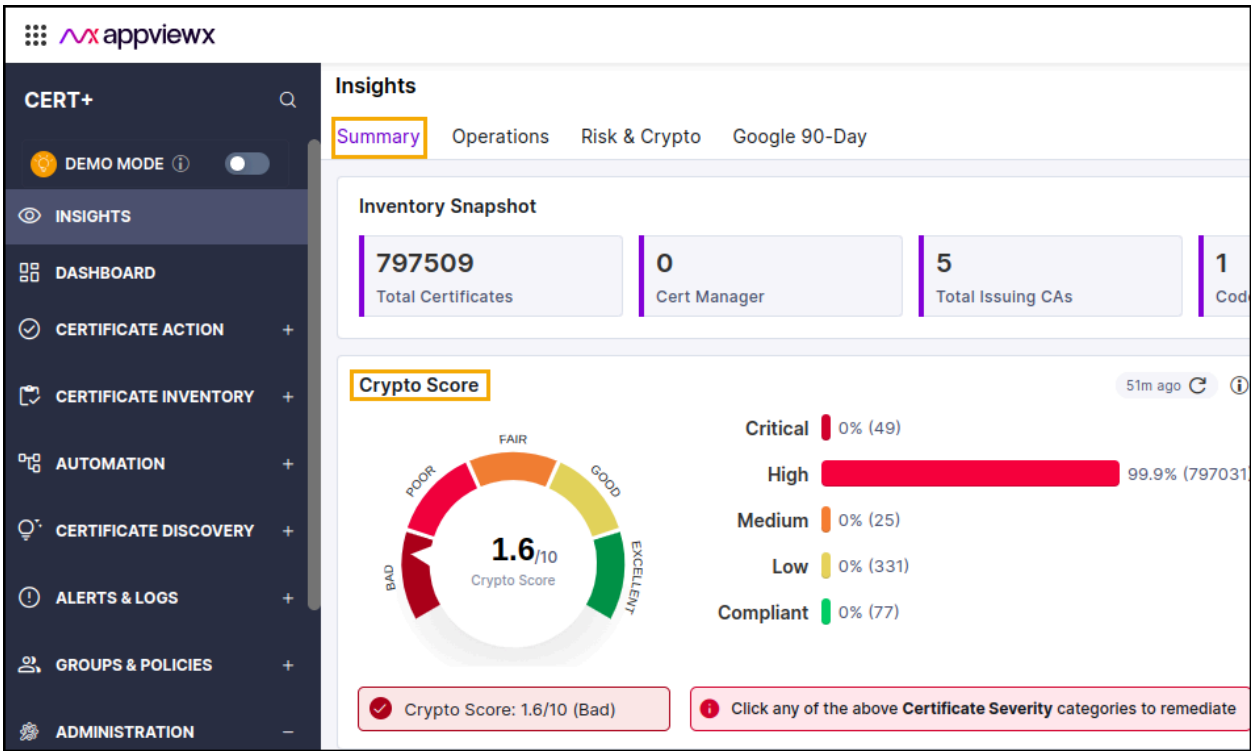


- **Total Certificates** - Displays the count of certificates such as Server, Client, and Code signing certificates.
- **Cert manager** - Displays the Up scaling tab.
- **Total Issuing CAs** - Total Issuing CAs report displays all the CA vendors that are currently managed or monitored.
- **Code Signing Certificates** - It displays the count of code signing certificates.
- **Total Devices** - The count of devices that are managed within AppViewX.

Crypto Score

The certificate score aligns with AppViewX compliance standards. This is a framework designed to streamline certificate management, assess foundational aspects, and gauge associated risks effectively.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

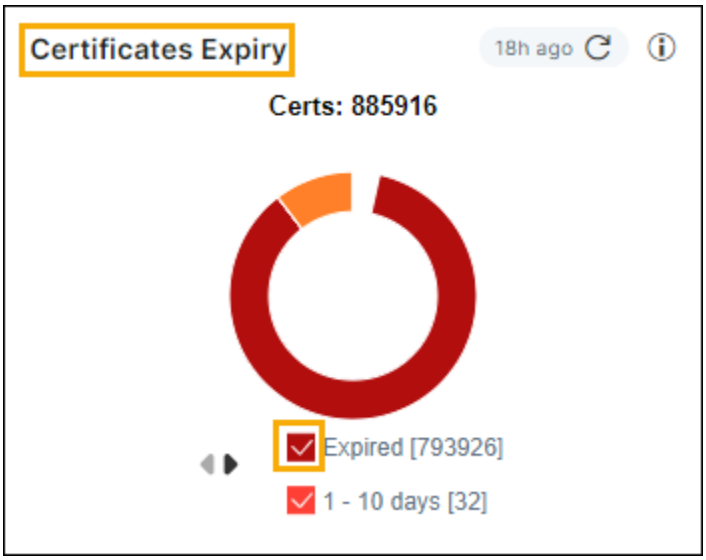


Certificate Expiry

The count of expired certificates such as Server, Client, and Code Signing certificates that are managed within AppViewX. You have the following options:

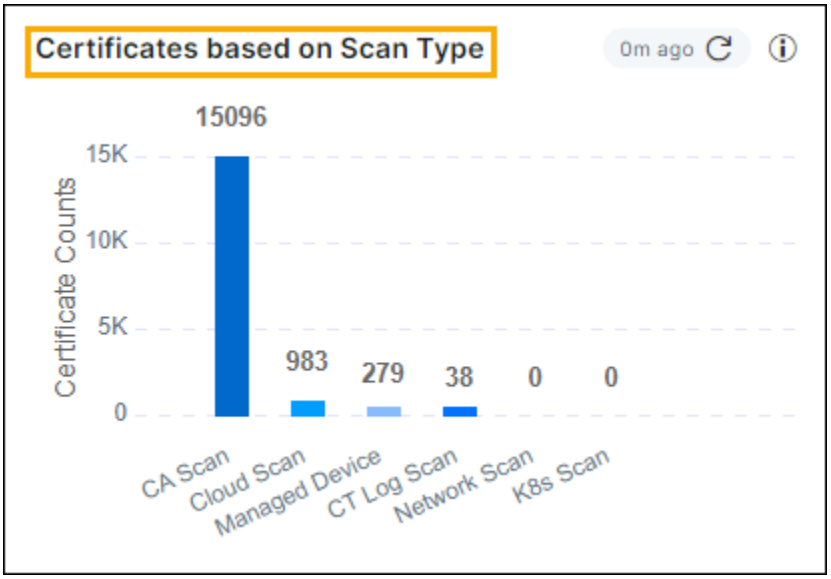
- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to intermediate page.
- Click the **Remediate** button to redirect to the Server/Client/Code signing certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Certificates based on Scan Type

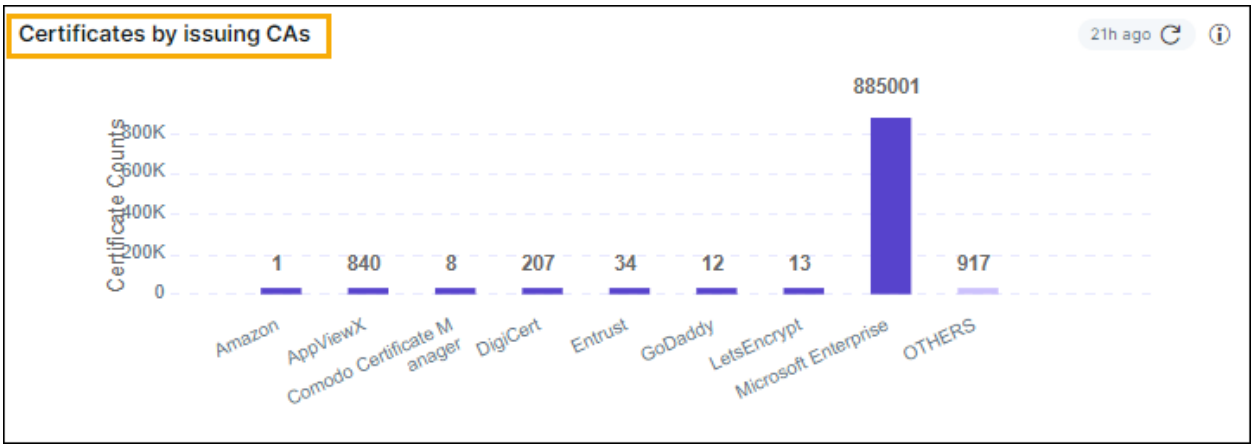
Certificates can be scanned and organized in various ways within the product. This widget provides a list of certificates scanned in each mode, tailored to the user's access. The X-axis represents the type of scan and Y-axis represents the number certificates per scan.



Certificates by issuing CAs

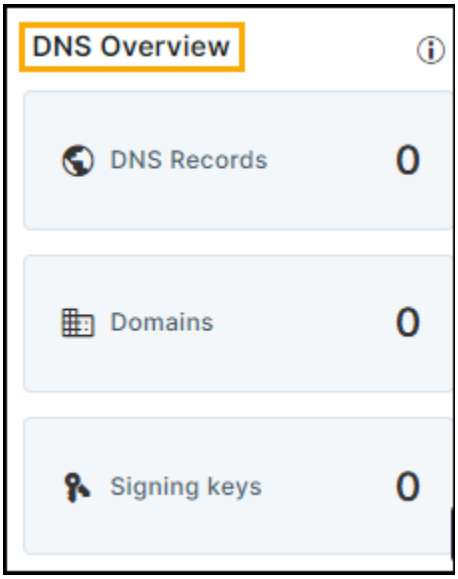
This report displays the count of issuing CAs. The X-axis represents the names of the vendors and Y-axis represents the number certificates per vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



DNS Overview

DNS Overview displays a comprehensive review and analysis of the internet domains and sub-domains the organization owns and manages. This includes an understanding of DNS records, domains, and signing keys that are utilized within the company's digital ecosystem.



- **Domains**: These are the main web addresses the organization owns. For example, appviewx.com.
- **Sub-domains**: These are subdivisions of the primary domain used for specific functions. For example, support.appviewx.com.
- **DNS Records**: DNS records are crucial components that help route internet traffic to the correct server.
- **Signing Keys**: A layer of security to DNS by enabling the verification of DNS responses. This helps protect against attacks like DNS spoofing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

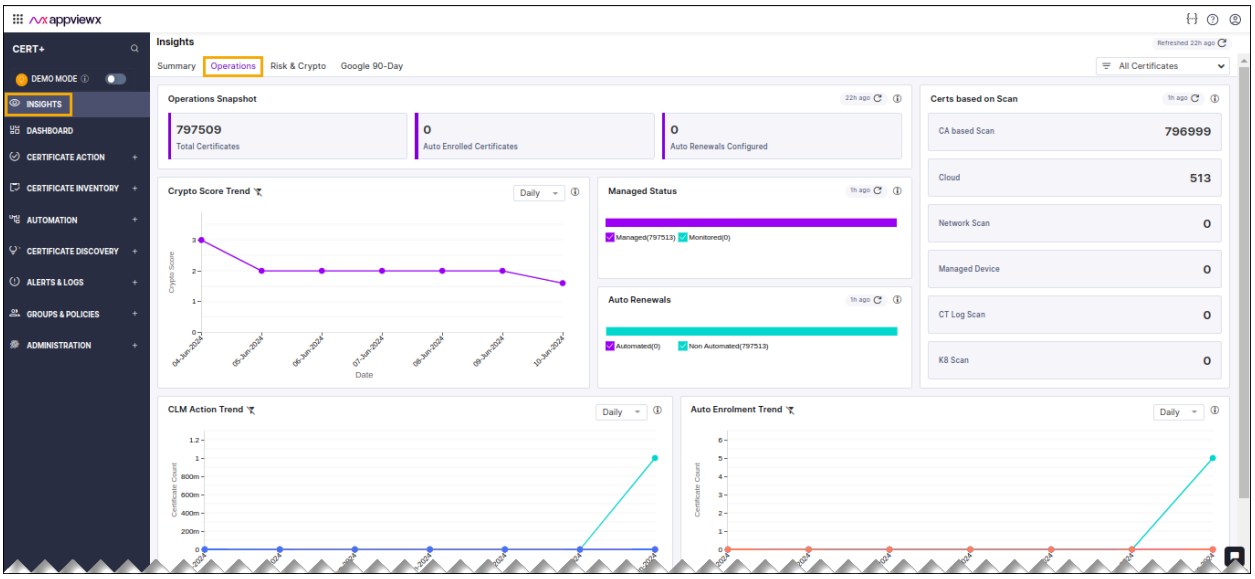
Threshold Limits

- For less than 100,000 certificates, live data will be displayed whenever the user navigates to the Insights page.
- For more than 100,000 certificates, a pre-calculated report will be shown with the last generated time indicated at the widget level.
- Users can click the widget level refresh to view the live data.

Insights Operations

The Insights Summary report presents a concise overview of the Operations Snapshot, Certs based on Scan, Crypto Score Trend, Managed Status, Crypto Score Trend, CLM Action Trend, Auto Renewals, and Auto Enrollment Trend managed within AppViewX. Click on any widget to access detailed information specific to that particular operations on the respective widgets popup. Within the popup window, you can view all the entries, export the content in the desired format if needed, and redirect to inventory. The Widgets within the Insights Summary report are:

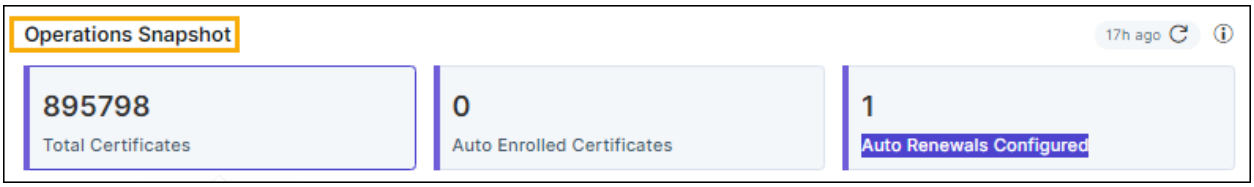
- **Operations Snapshot**
- **Certs based on Scan**
- **Managed Status**
- **Auto Renewals**
- **Crypto Score Trend**
- **CLM Action Trend**
- **Auto Enrolment Trend**



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operations Snapshot

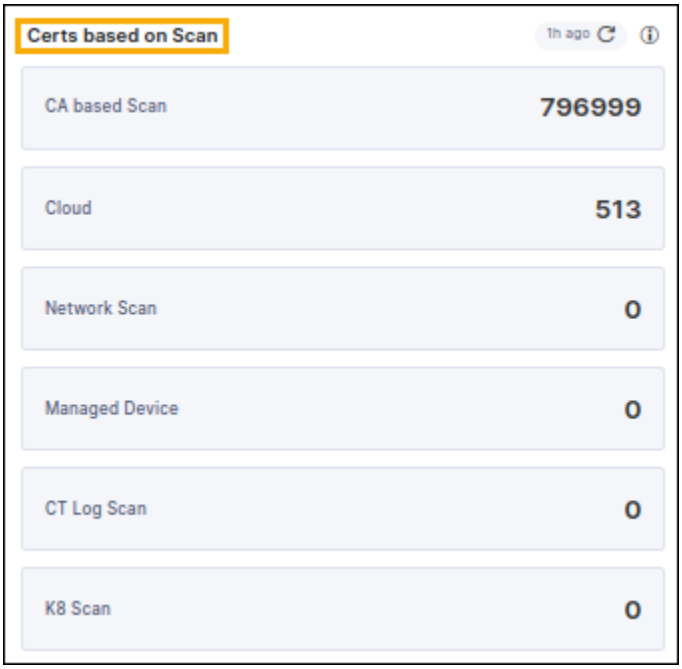
The Operations Snapshot widget displays the count of certificates, Auto Enrolled Certificates, and Auto Renewals Configured within AppViewX. The metrics within Operations Snapshot widget are:



- **Total Certificates** - Displays the count of certificates such as Server, Client, and Code signing certificates.
- **Auto Enrolled Certificates** - Displays the count of certificates that are enrolled using Auto Enrollment Protocol.
- **Auto Renewals Configured** - Displays the count of certificates currently configured for auto-renewal.

Certs based on Scan

This widget displays the count of certificates based on scan such as CA based scan, Managed device, CT Log scan, Cloud, Network Scan, External Tool, and K8s Scan.

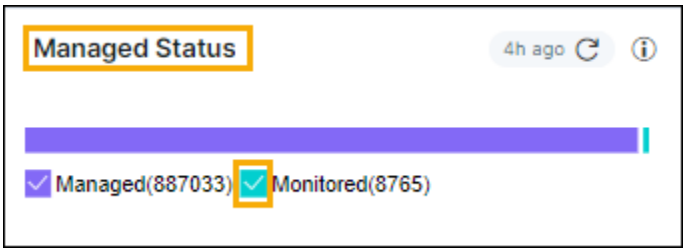


Managed Status

This widget shows the total count of certificates in both the managing and monitoring statuses. You have the following options:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

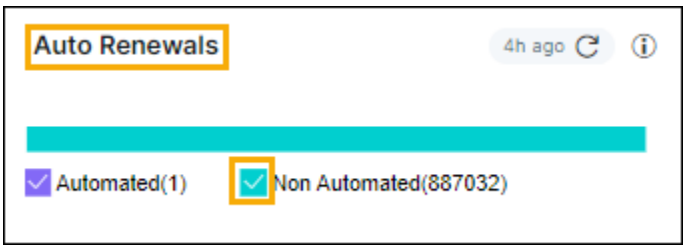
- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to intermediate page.
- Click the **Remediate** button to redirect to the Server/Client/Code signing certificate inventory.



Auto Renewals

This widget shows the total count of certificates in both the automated and Non automated. You have the following options:

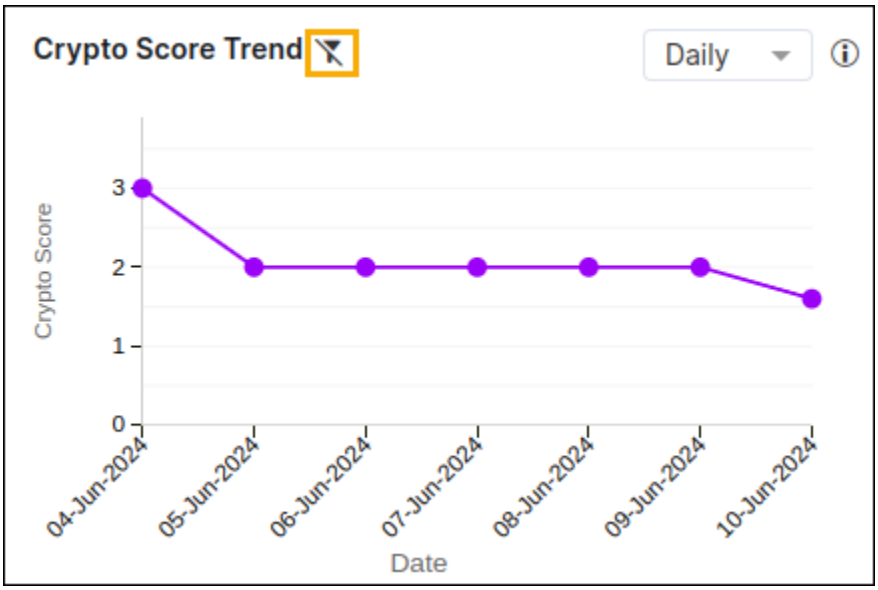
- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to intermediate page.
- Click the **Remediate** button to redirect to the Server/Client/Code signing certificate inventory.



Crypto Score Trend

This score indicates the security and condition of cryptographic components within a system, including certificates, encryption protocols, or cryptographic algorithms. You have the option to choose the trend chart format in various ways, including Daily, Weekly, Monthly, Quarterly, and Custom.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

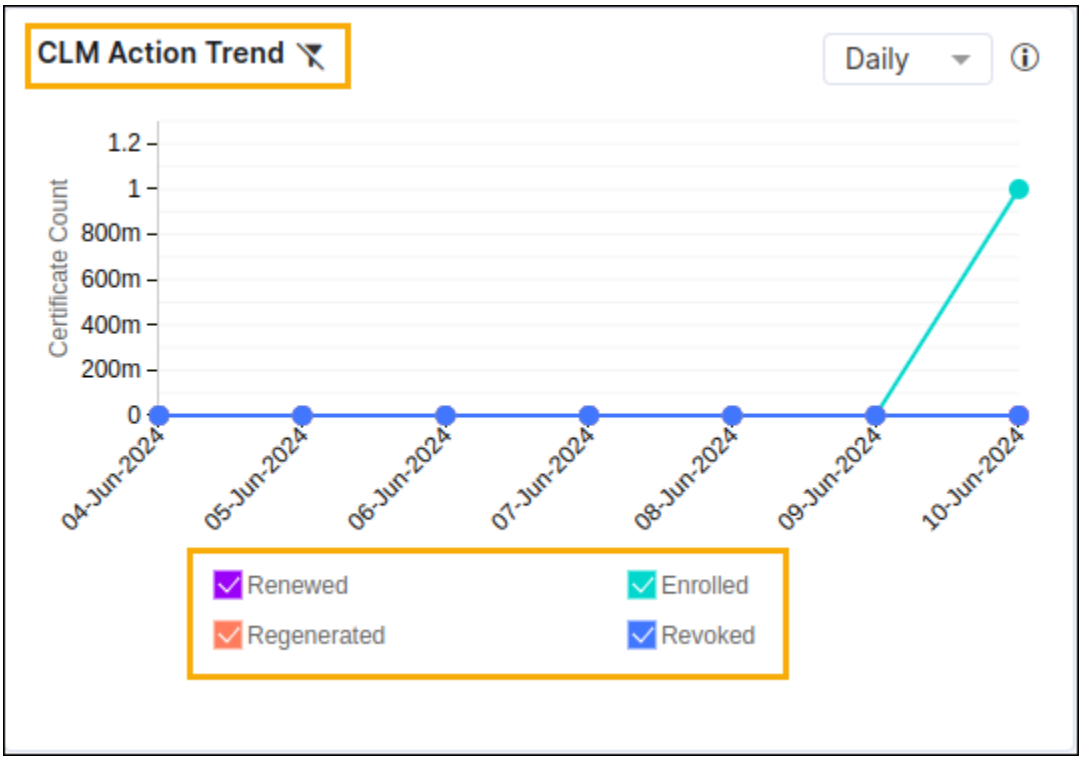


CLM Action Trend

This CLM action trend chart displays the count of renewed, enrolled, revoked, and regenerated certificates. You have the option to choose the trend chart format in various ways, including Daily, Weekly, Monthly, Quarterly, and Custom. You have the following more options:

- Select the check-box to view the specific portion, excluding unselected items.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

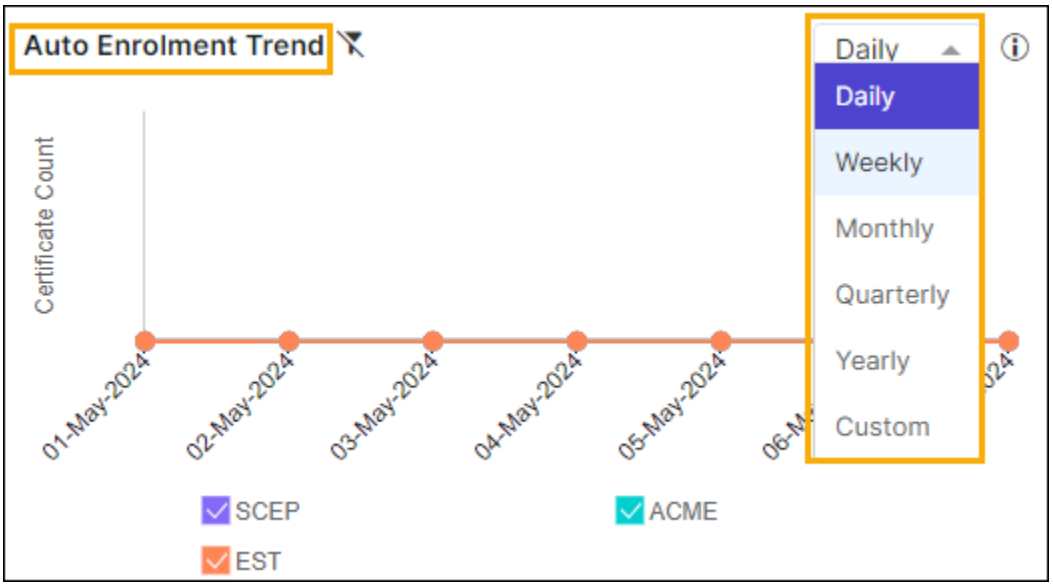


Auto Enrolment Trend

This trend displays the frequency or volume of certificates being automatically enrolled within a system. You have the option to choose the trend chart format in various ways, including Daily, Weekly, Monthly, Quarterly, and Custom. You have the following more options:

- Select the check-box to view the specific portion, excluding unselected items.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



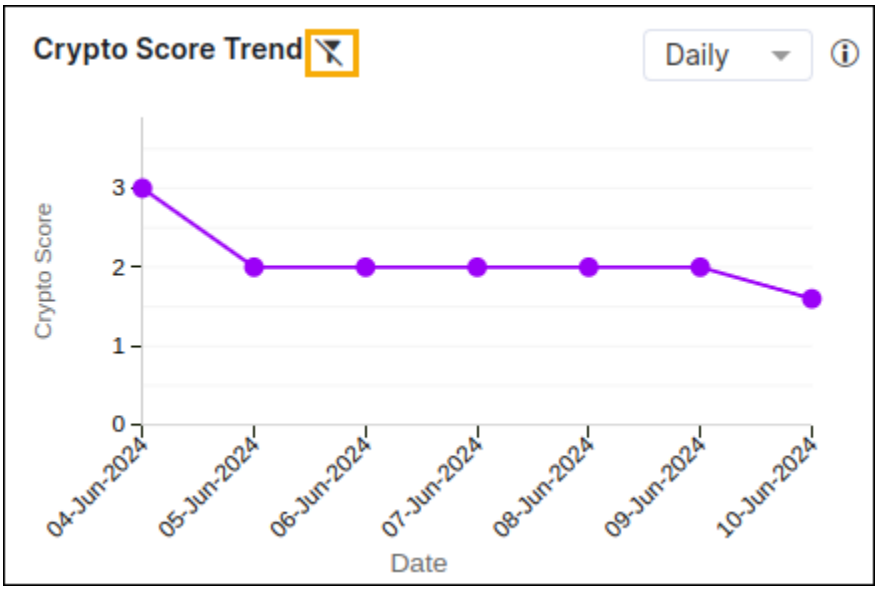
Threshold Limits

- For fewer than 100,000 certificates, live data will be displayed whenever the user navigates to the Insights page.
- For more than 100,000 certificates, a pre-calculated report will be shown with the last generated time indicated at the widget level.
- Users can click the widget level refresh to view the live data.

Trend Filter

It indicates that the group level filter is not applicable to this chart. The group level filter does not apply to the trend's filter and retains the same data for all users.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



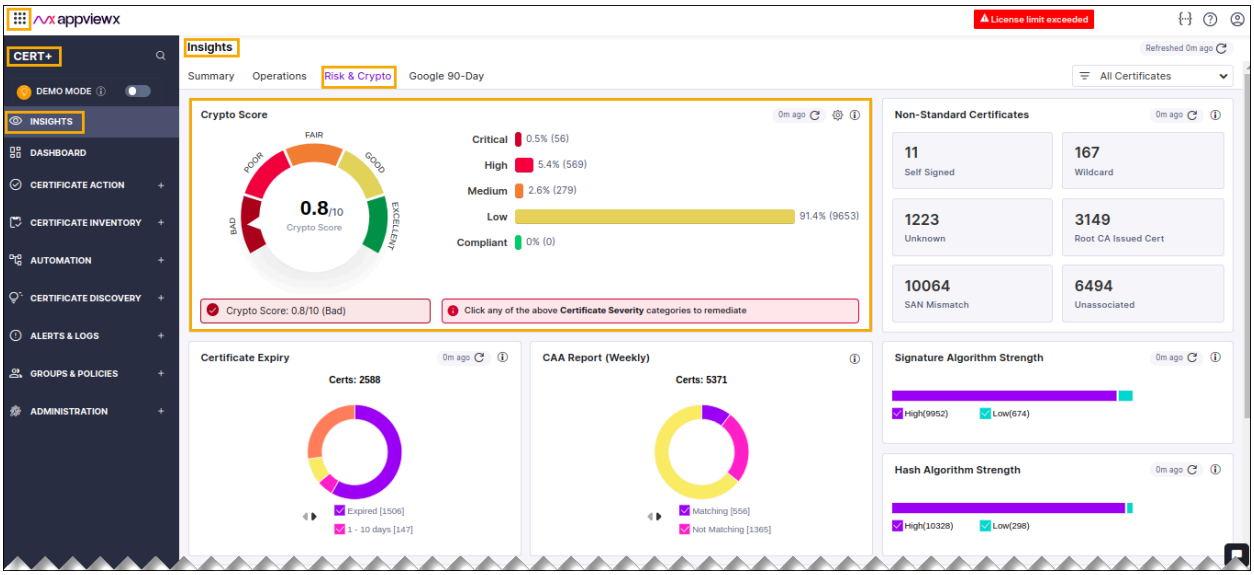
Insights Risk and Crypto

In Certificate Life Cycle Management, the "Crypto Score" typically refers to a metric or rating that assesses the security and health of cryptographic elements within the certificate ecosystem. This score evaluates factors such as certificate validity, strength of cryptographic algorithms, adherence to security best practices, and overall robustness of encryption protocols. It helps administrators monitor and maintain the security posture of certificates throughout their life cycle, identifying potential vulnerabilities or weaknesses that may need to be addressed.

The insights Risk and Crypto report presents a concise overview of the Crypto Score, Non-standard certificates, managed within AppViewX. Click on any widget to access detailed information specific to that particular operations on the respective widgets popup. Within the popup window, you can view all the entries, export the content in the desired format if needed, and redirect to inventory. The Widgets within the Insights Risk & Crypto report are:

- **Crypto Score**
- **Non-Standard Certificates**
- **Certificates Expiry**
- **CAA Report**
- **Signature algorithm strength**
- **Hash algorithm strength**
- **Crypto Score Trend**
- **Cipher Suite**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Crypto Score

The Crypto Score widget presents the average certificate score, including total score, critical risk certificates, high-risk certificates, medium-risk certificates, low-risk certificates, and good certificates, all based on the configured certificate compliance.

Crypto Score Calculation

The Crypto Score for a set of certificates is determined by combining each certificate's base score with the weighted priorities assigned to specific risk categories. Below is a step-by-step breakdown of the calculation process:

- **Determine the Base Score**: Each certificate is assigned a base score based on its attributes and usage. This score reflects factors such as:
  - Validity period
  - Key algorithm
  - Key size
  - Usage in applications or devices (for example, used for authentication).
- **Assign Priority Weights**: Each certificate is placed into a priority group based on its characteristics. Different priority groups have different weights:
- Each certificate is categorized into a priority group based on its characteristics, with each group representing a specific level of risk. The defined priority groups and their associated risks are as follows:
  - **Priority 0**: Expired/Revoked Certificates, Self-Signed Certificates, Wildcard Certificates
  - **Priority 1**: Weak Key Size, Weak CA Key Size

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Priority 2**: Weak Hashing Algorithms
- **Priority 3**: Unauthorized Certificate Authorities (CAs).

Each priority group is assigned a weight, which is factored into the overall Crypto Score calculation.

Calculate the Individual Score

The individual score for a certificate is calculated using the following formula:

Individual Score = ∑ (Priority Weight × Base Score)

The score is the sum of the products of each applicable priority group's weight and the certificate's base score, providing a weighted assessment of the certificate's overall risk.

Classify Certificate Severity

Based on the calculated individual score, the certificate is classified into one of the following **severity levels**:

- **Critical (>=8)**
- **High (7.9-5)**
- **Medium (4.9-3)**
- **Low (2.9-1)**
- **Good (0.9-0)**.

After classification, certificates are grouped by severity for further aggregation.

Example Calculations

- Example 1: Weak Certificate

  Attributes:

  - Wildcard certificate (**Priority 0**)
  - Weak key size (**Priority 1**)
  - Weak hashing (**Priority 2**).

  Base Scores:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Wildcard: 5
- Weak key size: 3
- Weak hashing: 2

Priority Weights:

- Priority 0: 3
- Priority 1: 2
- Priority 2: 1

Calculation:

Individual Score = (3 × 5) + (2 × 3) + (1 × 2)

= 15 + 6 + 2

= 23

As the individual score is **23**, which is greater than **8**, the certificate falls into the **Critical** severity range and is categorized as **Critical**.

Example 2: Strong Certificate

Attributes:

- Valid
- Strong key size
- Strong hashing

Priority Weights:

- Priority 0: 0.1
- Priority 1: 0
- Priority 2: 0

Calculation:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Individual Score = (0.1 × 5) + (0 × 3) + (0 × 2)

= 0.5 + 0 + 0

= 0.5

Since the individual score is **0.5**, which is less than **0.9**, the certificate is categorized as **Good**.

Aggregate Overall Crypto Score

The overall Crypto Score is calculated by aggregating all certificates based on their severity levels using a logarithmic scale.

- The final Crypto Score ranges from **1 to 10**.

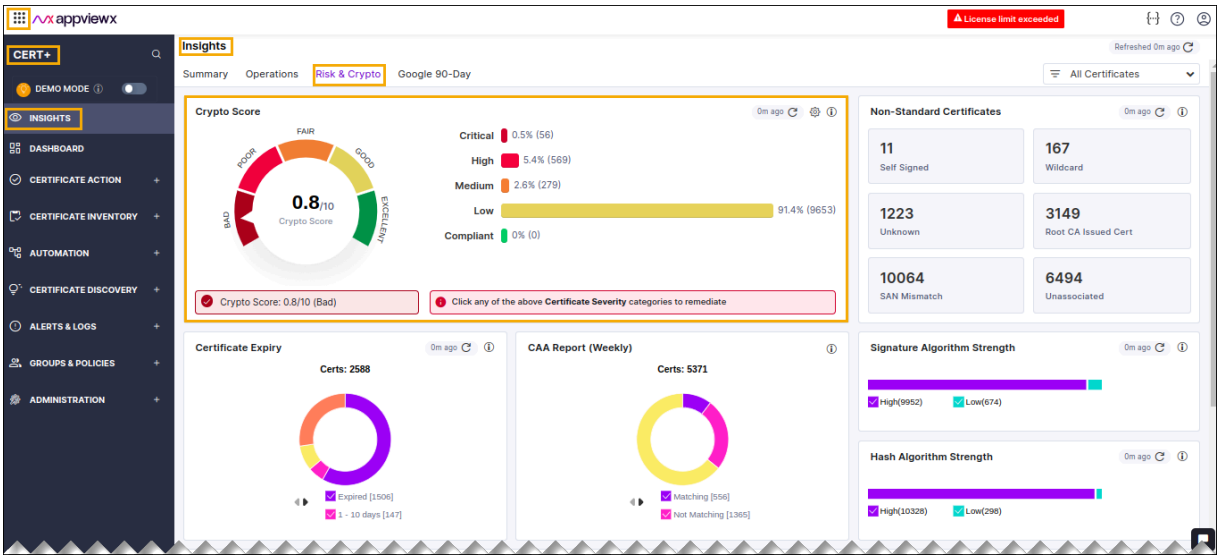
If the calculated score exceeds 10, it is capped at **10**.

Crypto Score Configuration

To configure the crypto score, do the following steps.

1. Go to (**Menu**) > **CERT+** > **INSIGHTS**.

   The Insights window is displayed.



2. Click **Risk & Crypto**.

   The **Rick & Crypto** score page is displayed.

3. In the **Crypto Score** section, click the (Settings Gear) icon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Crypto Score Configuration** page is displayed.

The field description for configuring the crypto score.

Field	Description
*Strongest Algorithm	Select the strongest algorithm to ensure that the data security and integrity in various cryptographic operations, such as encryption, digital signatures, and authentication. The available options are: • *RSA • *DSA • *EC.
*Strongest Hash	Select the strongest hash from the list.
*Prioritize score components	Select components based on priority level to calculate the crypto score. You can select maximum 3 components in a single priority list. • Priority 0 • Priority 1 • Priority 2 • Priority 3
**: Mandatory fields*	

4. Click **Save**.

Non-Standard Certificates

Displays a report detailing the count of non-standard certificates in the following categories:

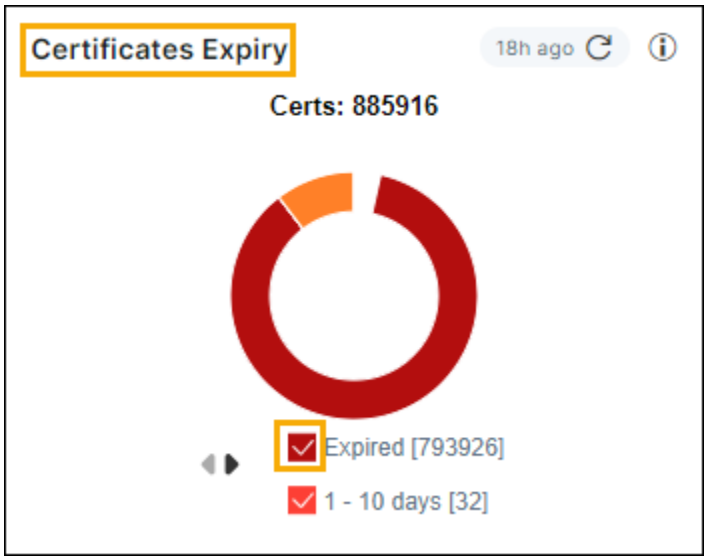
- Self-Signed
- Wildcard
- Unknown
- Root CA Issued Certificates
- SAN Mismatch
- Unassociated Certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificates Expiry

The Expiry Certificate widget shows the number of certificates set to expire within the next 1 to 10 days. Additionally, it indicates the count of certificates that have already expired. You have the following options:

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the **Certificates Expiry :: Expired** and ×**Certificates Expiry :: 1 - 10 days**, and to the remaining pages.
- Click the **View in inventory** tab that redirects to the **Certificates Expiry** page.

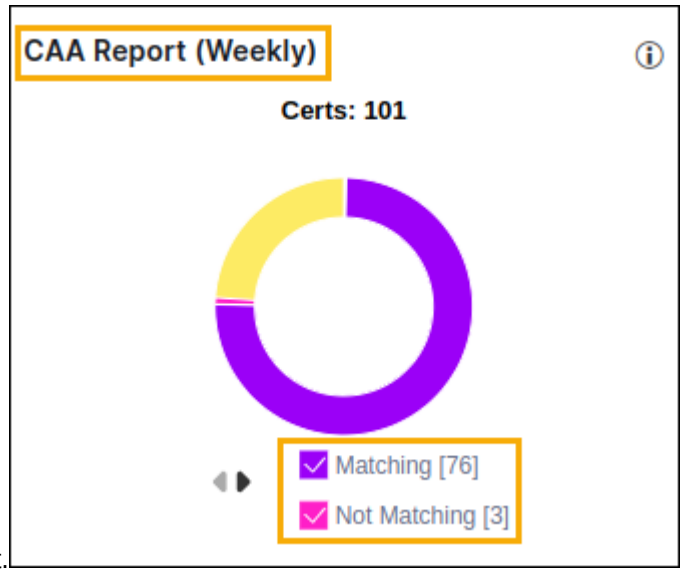


CAA Report

This report shows the count of certificates with and without CAA records in the inventory. You have the following options:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

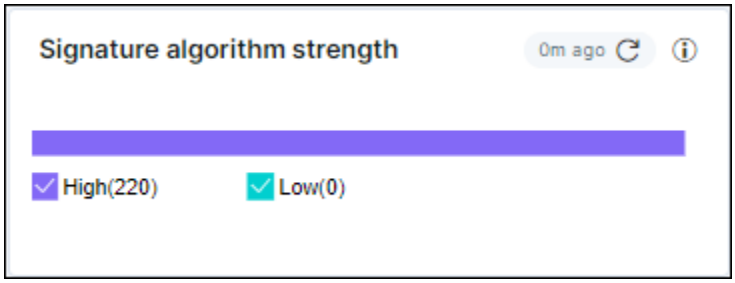
- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the respective inventory report.



Signature algorithm strength

Displays the count of certificates based on their signature algorithm strength, categorized as either high or low. A higher signature algorithm strength indicates stronger cryptographic algorithms, which are more resistant to attacks and tampering, thus enhancing the overall security posture of the system. You have the following options:

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the chart to redirect to the respective report.

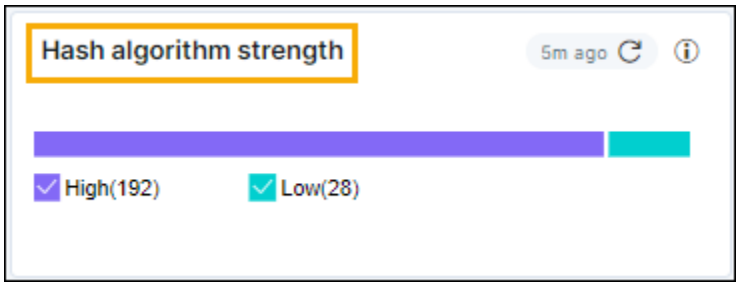


Hash algorithm strength

Displays the count of certificates based on their hash algorithm strength, categorized as either high or low. A higher signature hash strength indicates stronger cryptographic algorithms, which are more resistant to attacks and tampering, thus enhancing the overall security posture of the system. You have the following options:

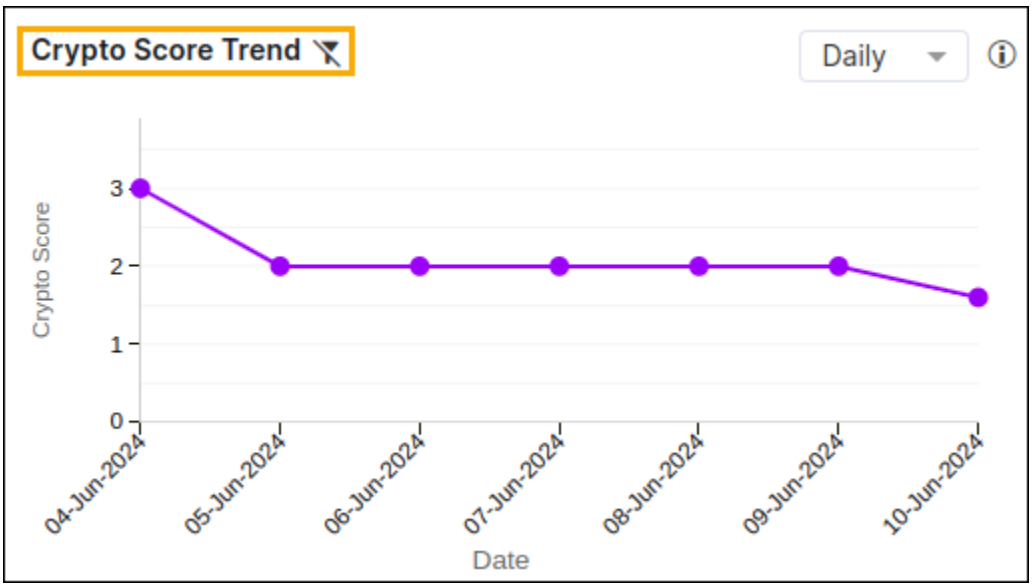
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the chart to redirect to the respective report.



Crypto Score Trend

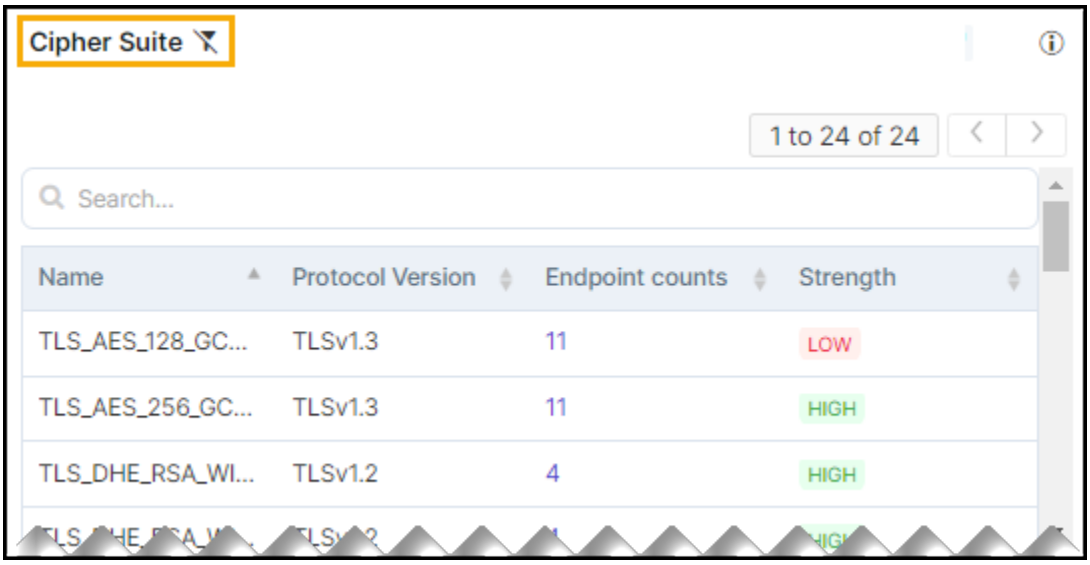
This score indicates the security and condition of cryptographic components within a system, including certificates, encryption protocols, or cryptographic algorithms.



Cipher Suite

The Cipher report in the Insights dashboard no longer uses a separate strength mapping configuration. Instead, it now references the strength mapping defined under Administration > General Settings > Cipher Settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Threshold Limits

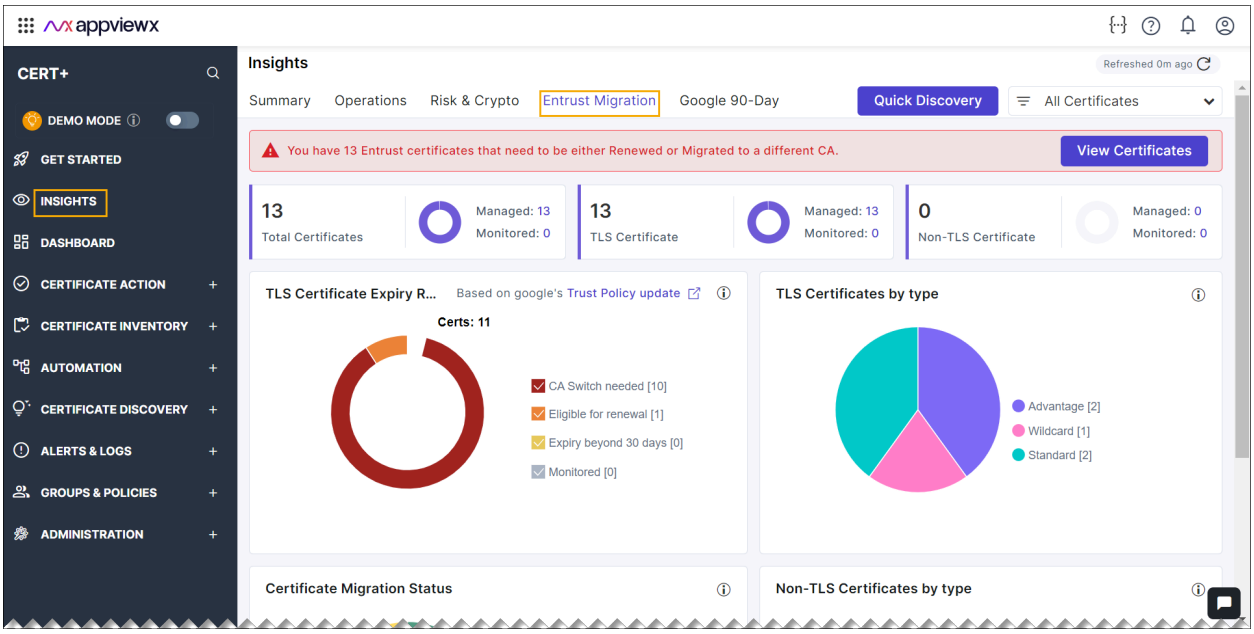
- For fewer than 100,000 certificates, live data will be displayed whenever the user navigates to the Insights page.
- For more than 100,000 certificates, a pre-calculated report will be shown with the last generated time indicated at the widget level.
- Users can click the widget level refresh to view the live data.

Insights Entrust Migration

The Entrust Migration Insights Dashboard is designed to provide a comprehensive view of all certificates issued by Entrust. It allows users to monitor, manage, and migrate their certificates effectively. The dashboard is segmented into various sections and widgets, each offering specific insights and actions related to Entrust-issued certificates. This dashboard aims to streamline the management of Entrust-issued certificates, ensuring timely renewals and efficient migration, while keeping users informed and in control of their certificate landscape.

- TLS Certificate Expiry Report
- TLS Certificates by Type
- Certificate Migration Status
- Non-TLS Certificates by Type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Purpose of Entrust Migration Dashboard

Real-Time Data Display:

- Total number of Entrust-issued certificates.
- Certificates eligible for renewal or needing migration.
- Successfully migrated certificates and those still pending.
- Active certificates currently in use.

Direct Actions:

- Users can renew certificates or initiate their migration directly from the dashboard.

Real-Time Updates:

- The dashboard features real-time updates, with a refresh button at the top indicating the last refresh time.
- Auto-refresh occurs every 12 hours.

Detailed Auditing:

- Comprehensive logging and auditing for tracking all certificate-related activities.

Certificate Validity:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Only valid certificates are displayed, excluding expired or revoked Entrust certificates.

Alert Message

A red banner at the top alerts you that there are 13 Entrust certificates, which has to be either renewed or migrated to a different Certificate Authority (CA).

Title Bar

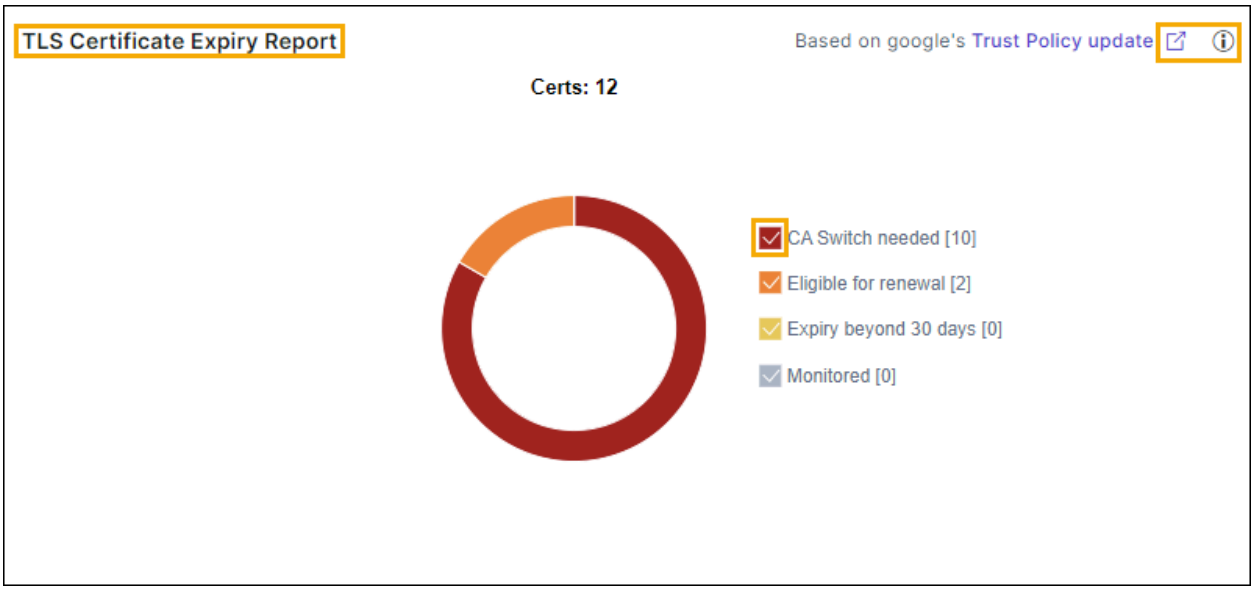
The title bar offers a concise summary of all certificates issued by Entrust. It displays three interactive widgets:

• Total Entrust Certificates
• TLS Certificates
• Non-TLS Certificates.

Each widget displays certificate data, covering both Managed and Monitored certificates.

TLS Certificate Expiry Report

This widget provides a detailed report on certificates that need to be migrated or renewed.



Categories include:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **CA Switch Needed**: This includes certificates that need to be switched to a different Certificate Authority from Entrust, as they expire after November 30th, 2024.
- **Eligible for Renewal**: This includes certificates that are set to expire within the next 30 days, up until November 30th, 2024.
- **Not Eligible for Renewal**: This includes certificates that expire more than 30 days from now, until November 30th, 2024.

> **Note:** Entrust permits certificate renewals only for those expiring within 30 days.

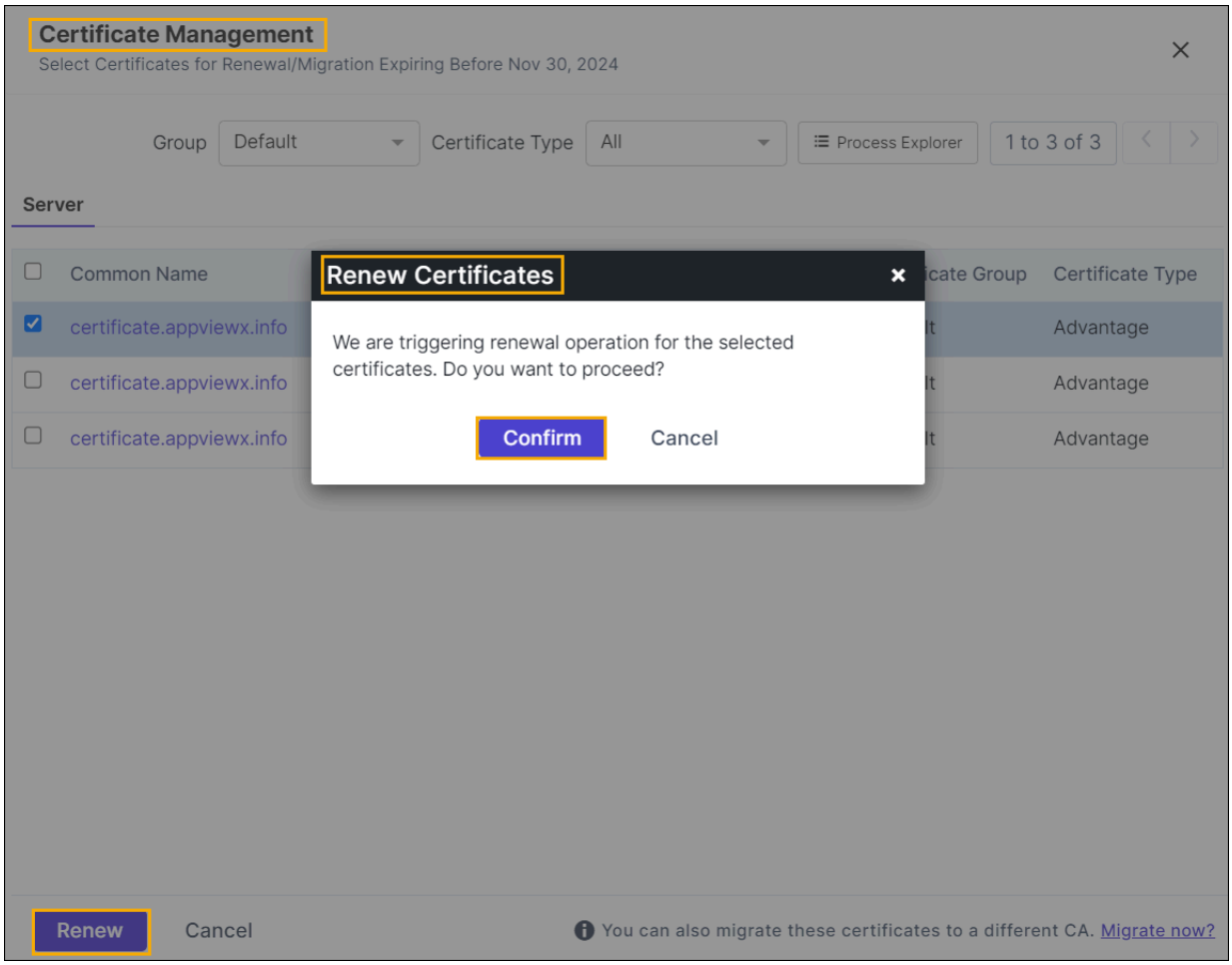
- **Monitored**: This includes certificates that are currently in Monitored status in the inventory. These certificates will need to be moved to Managed status in order to perform a CA switch or renewal.

> **Note:** Google's Entrust Distrust update, any certificate issued up until October 31st, 2024, is considered valid. Since Entrust only allows renewing certificates within 30 days of their expiry, certificates expiring by November 30th, 2024, can be renewed and remain valid. However, any certificate expiring after this date must be switched to a different Certificate Authority.

- **Link Icon:** Explains the impact of Google's distrust of Entrust-issued certificates and includes a link for more details.

- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to **Certificate Management** page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



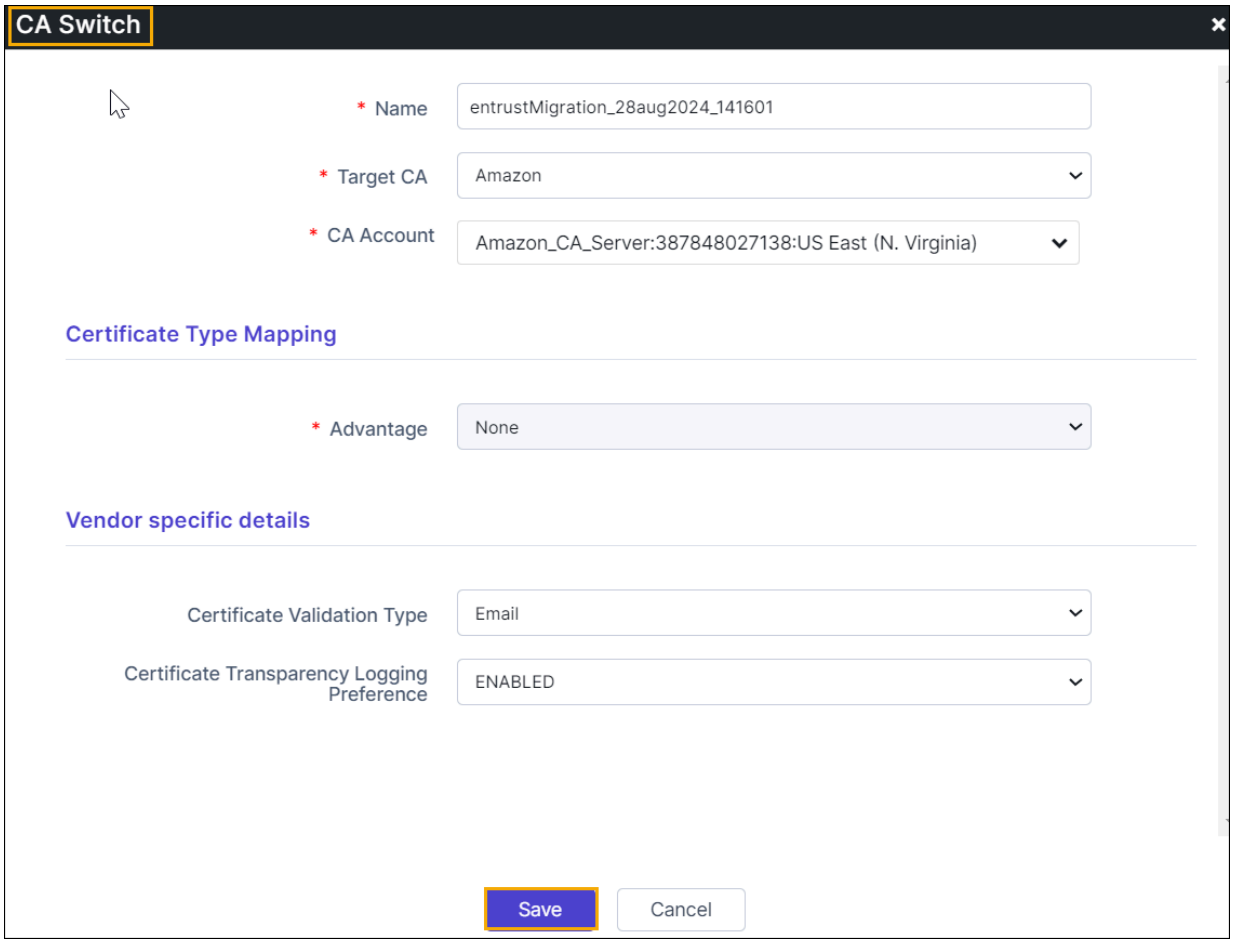
- **Group**: A dropdown labeled "Group" is set to "Default".
- **Certificate Type**: Another dropdown labeled "Certificate Type" is set to "All".
- **Process Explorer**: There is a button labeled "Process Explorer", likely used for detailed analysis or tracking of certificate processing.
- **Pagination**: The interface indicates that the user is viewing items 1 to 8 out of a total number, with navigation arrows for moving between pages.

- The main section of the interface displays a table listing certificates with the following columns:
- **Common Name**: The domain name associated with each certificate (for example, `poshacme.appviewwx.net`).
- **Expiry Date-Time**: The exact date and time when each certificate will expire (for example, 14/02/2025 17:21).
- **Discovery Source**: The source from which the certificate was discovered (for example, `MicrosoftServer`).
- **Applications Associated**: This column is likely meant to display the applications linked to each certificate, though in the image it appears empty.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

  - **Certificate Group**: Indicates the group to which each certificate belongs, set to "Default" in all cases.
  - **Certificate Type**: Also set to "Default" for each entry, this column categorizes certificates by their type.
- Each row has a check box to the left of the common name, allows you to select individual certificates for migration or further actions.
- At the bottom of the interface, there are options to **Renew** or **Cancel**. The **Renew** button is prominently displayed, indicating that the user can initiate the renewal process for the selected certificates if the **Eligible for renewal** certificate pie chart selected.
  - Click **Renew**, the **Renew Certificates** pop-up window appears with message as "We are triggering renewal operation for the selected certificates. Do you want to proceed?".
  - Click the **Confirm** button, the certificate gets renewed and the message is displayed as "We have successfully initiated the Renewal of 1 certificates" along with the **Click to View** link.
  - To see the renewed certificate in the **Renew Certificate** page, click the **Click to View** link that redirects to **Insights** > **Entrust Migration** > **Renew Certificate** view page.
- Click the **Cancel** button to discard the current changes and exit the form without saving.
- Click the certificate link to redirect to the Server certificate holistic view.
- A note at the bottom of the page indicates that user can also migrate the selected certificates to a different Certificate Authority (CA), with a link provided ("Migrate now?") for further action. Click the **Migrate now?** button that redirects to CA Switch page. For more details about CA Switch, refer the below steps.
- **CA Switch**: At the bottom of the interface, there are options to **Switch CA** or **Cancel**. The **Switch CA** button is prominently displayed, indicating that the user can initiate the CA Switch (migration) process for the selected certificates, if the **Eligible for CA Switch needed** certificate pie chart selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field descriptions for the CA Switch parameters

Fields	Description
***Name**	**Default**: Selected certificate name for the CA switch. The name of the migration task is specified as "entrustMigration_ 28aug2024_130633." This includes the date and time when the migration task was created.
***Target CA**	**Default**: Amazon. The dropdown menu shows that **Amazon** is selected as the target Certificate Authority to which the certificates will be migrated by default. The available options are: • **Amazon** • **Sectigo (Comodo Certificate Manager)**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• **Digicert** • **GlobalSign** • **Trustwave**
***CA Account**	This field is a dropdown menu, prompting the user to select an account associated with the chosen CA. **Note:** This field appears only if the **Amazon** selected in the target CA dropdown list.
***Settings**	This field is a dropdown menu, prompting the user to select an account associated with the chosen CA. **Note:** This field appears only if anyone of the **Sectigo (Comodo Certificate Manager)**, **Digicert**, **GlobalSign**, or **Trustwave**CA selected in the target CA dropdown list.
***Division**	**Default**: AppViewX Inc. Select the division from the dropdown list. The available options are: • **AppViewX Inc.** • **TestDivision** **Note:** This field appears only if the **Digicert** selected in the target CA dropdown list.
Certificate Type Mapping	
***Advantage**	Under the "Certificate Type Mapping" section, there is a dropdown menu labeled "Advantage," where "None" is selected. This allows users to map specific certificate types from the source CA to equivalent types in the target CA.
Vendor Specific Details	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This field appears only if anyone of the **Amazon**, **Digicert**, or **GlobalSign** CA selected in the target CA dropdown list.
Certificate Validation Type	**Default**: Email. The dropdown menu under this section shows "Email" as the selected validation type. The available options are: • **Email**: This indicates that email validation will be used for the certificates during the migration process. • **DNS**: his indicates that DNS validation will be used for the certificates during the migration process. **Note:** This field appears only if the **Amazon**, , CA selected in the target CA dropdown list.
Certificate Transparency Logging Preference	**Default**: ENABLED. The preference for Certificate Transparency Logging is set to **ENABLED**, meaning that the certificates will be logged in publicly accessible Certificate Transparency logs. **Note:** This field appears only if the **Amazon** CA selected in the target CA dropdown list.
***Server Type**	**Default**: Apache. Select the type of server from the dropdown list. This field determines the type of server environment in which the certificate will be used. **Note:** This field appears only if the **Digicert** CA selected in the target CA dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Payment Method**	**Default**: Bill To Account Balance. Select the type of method from the dropdown list. This field specifies how the payment for the service will be handled. "Bill To Account Balance" suggests that the charges will be deducted from a pre-existing account balance, possibly linked to the user's account with the vendor. The available methods are: • Bill To Account Balance • Bill To Default Credit Card. **Note:** This field appears only if the **GlobalSign** CA selected in the target CA dropdown list.
***Domain Admin Email**	**Default**: hostmaster. Select the type of domain admin email from the dropdown list. **Note:** This field appears only if the **Digicert** CA selected in the target CA dropdown list.
*: Mandatory fields	

- Click **Save**.

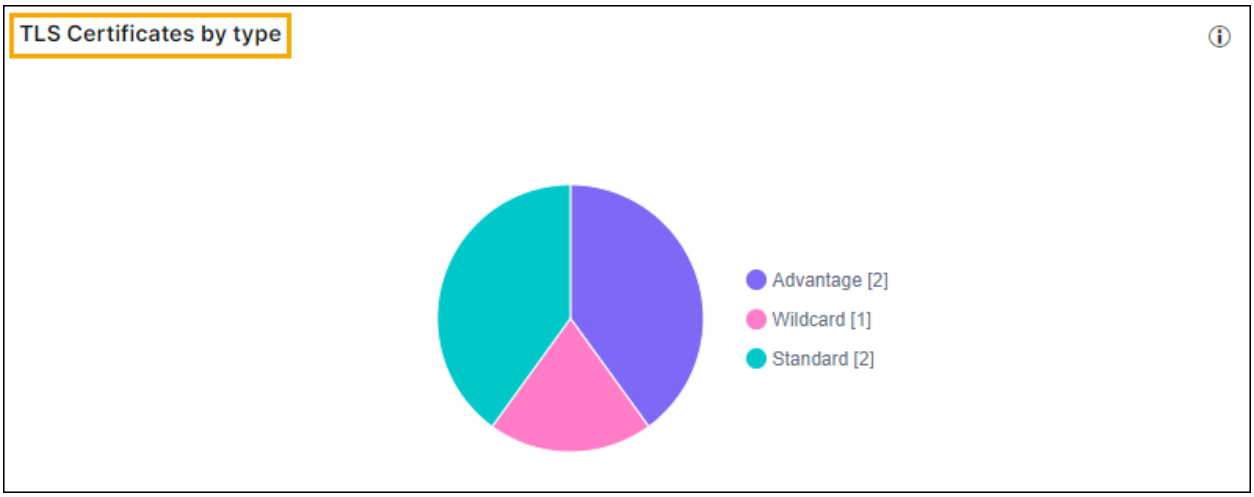
  The popup message appears as "<certificate name> saved" in the **CA Switch Summary** page.

- Click the **Cancel** button to discard the current changes and exit the form without saving.
- Select the checkbox for the certificate that you want to migrate CA, and then click **Submit**.

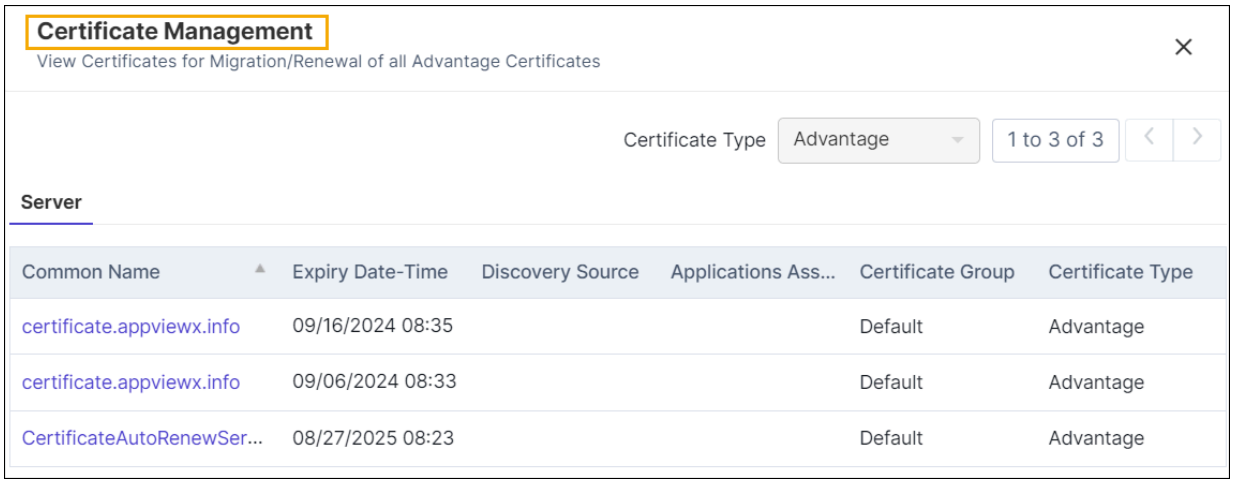
TLS Certificates by Type

This chart visually represents the distribution of TLS certificates based on their types. There are three distinct categories of certificates, each represented by a different color. The chart provides a quick visual summary of how many TLS certificates belong to each type such as **Standard**, **Advantage**, and **Wildcard**. Provides a drilldown option for more detailed insights, excluding certificates that have already been migrated or are in progress

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to **Certificate Management** page.

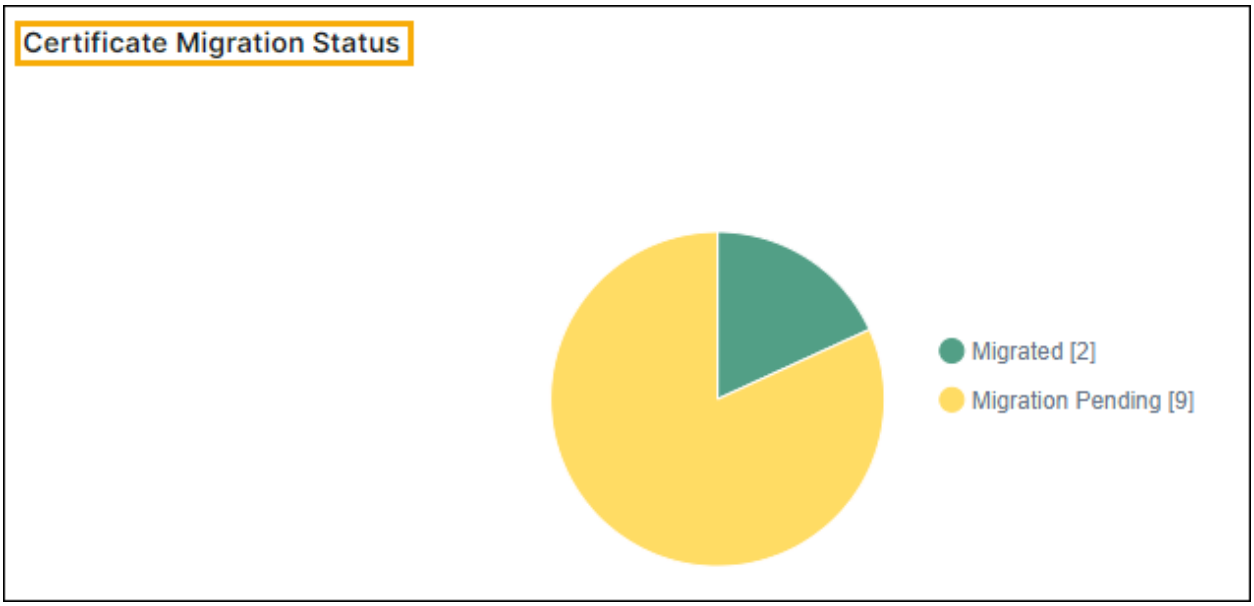


  - **Certificate Type**: Another dropdown labeled "Certificate Type" is set to "Advantage".
  - **Common Name**: The domain name associated with each certificate (for example, `poshacme.appviewwx.net`).
  - **Expiry Date-Time**: The exact date and time when each certificate will expire (for example, 14/02/2025 17:21).
  - **Discovery Source**: The source from which the certificate was discovered (for example, `MicrosoftServer`).
  - **Applications Associated**: This column is likely meant to display the applications linked to each certificate, though in the image it appears empty.
  - **Certificate Group**: Indicates the group to which each certificate belongs, set to "Default" in all cases.
  - **Certificate Type**: Also set to "Default" for each entry, this column categorizes certificates by their type.
- Click the certificate link to redirect to the Server certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

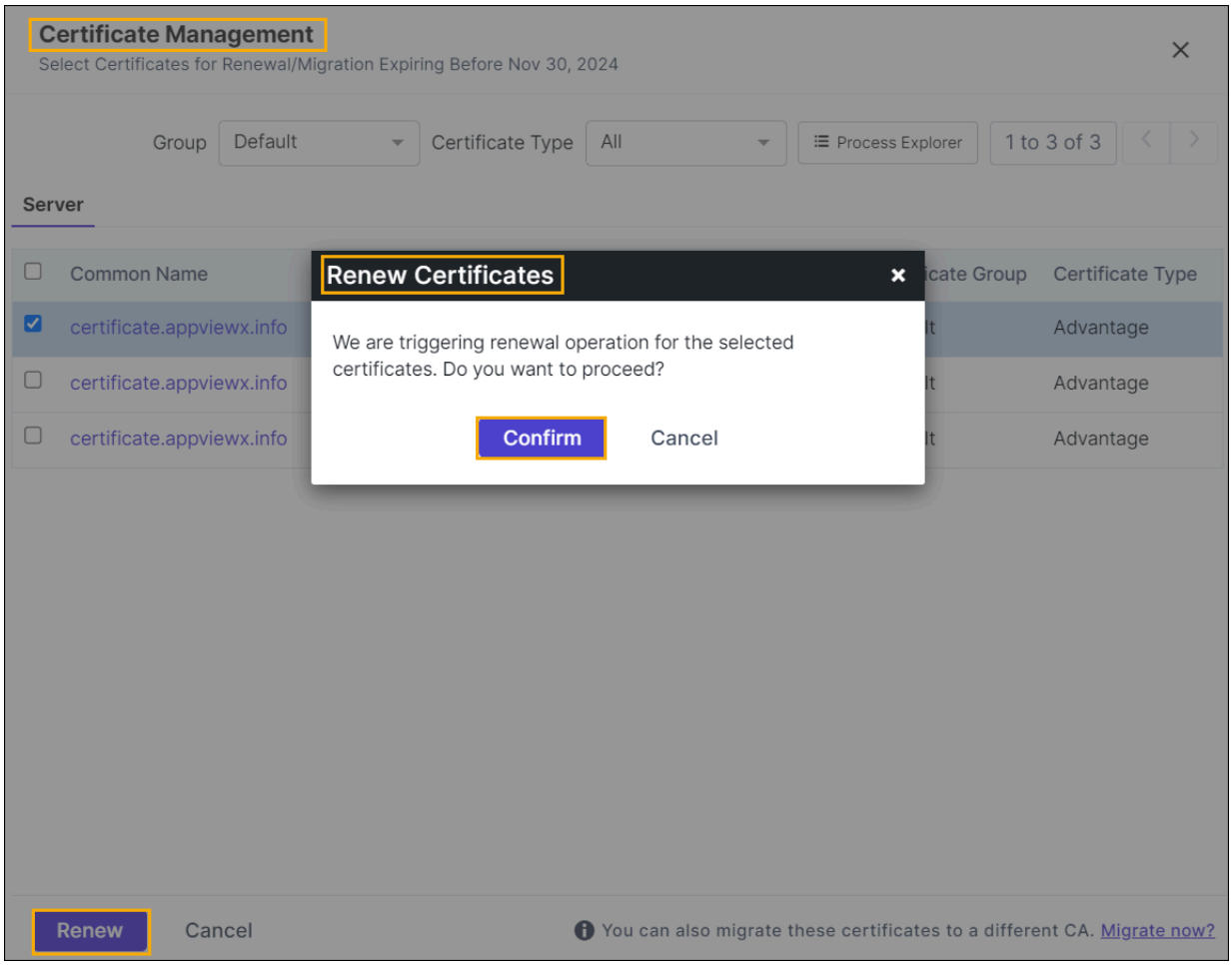
Certificate Migration Status:

Tracks the progress of Entrust certificate migration, showing how many have been migrated or are pending. Offers insights into the migration process and the status of certificates.



- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to **Certificate Management** page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



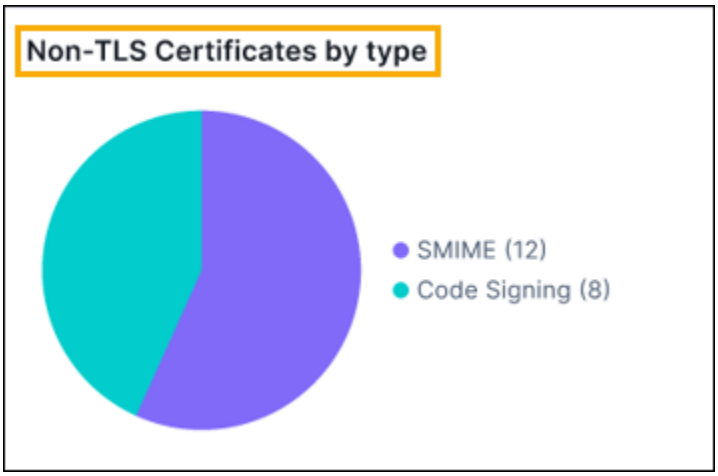
- **Certificate Type**: Another dropdown labeled "Certificate Type" is set to "All".
- **Common Name**: The domain name associated with each certificate (for example, `poshacme.appviewwx.net`).
- **Expiry Date-Time**: The exact date and time when each certificate will expire (for example, 14/02/2025 17:21).
- **Discovery Source**: The source from which the certificate was discovered (for example, `MicrosoftServer`).
- **Applications Associated**: This column is likely meant to display the applications linked to each certificate, though in the image it appears empty.
- **Certificate Group**: Indicates the group to which each certificate belongs, set to "Default" in all cases.
- **Certificate Type**: Also set to "Default" for each entry, this column categorizes certificates by their type.

• Click the certificate link to redirect to the Server certificate holistic view.

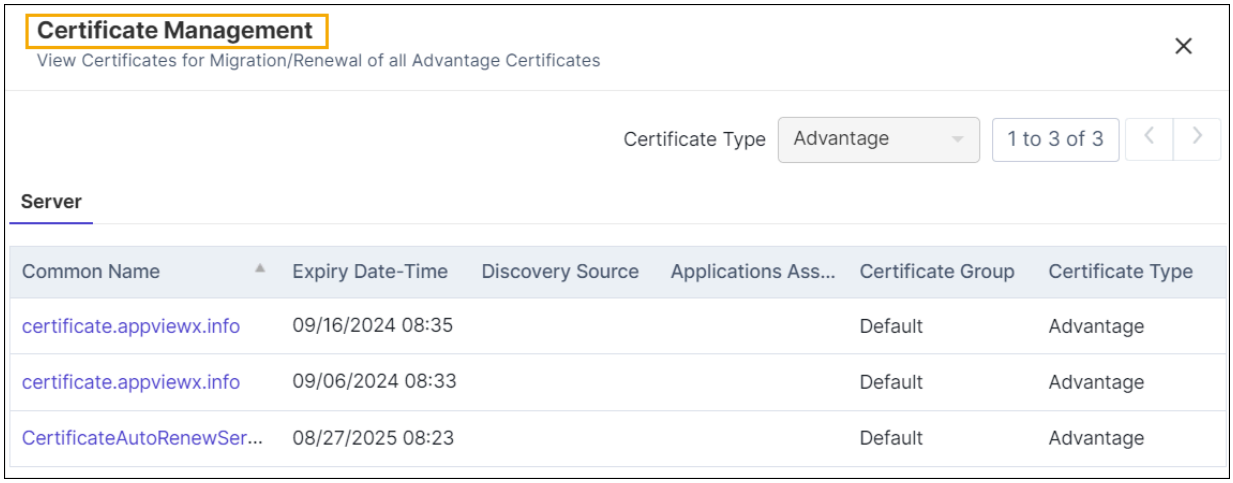
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Non-TLS Certificates by Type

Categorizes and displays Non-TLS Entrust certificates and excludes already migrated or in-progress certificates.



- Select the check-box to view the specific portion, excluding unselected items.
- Click the pie chart to redirect to **Certificate Management** page.



- **Certificate Type**: Another dropdown labeled "Certificate Type" is set to "Advantage".
- **Common Name**: The domain name associated with each certificate (for example, `poshacme.appviewwx.net`).
- **Expiry Date-Time**: The exact date and time when each certificate will expire (for example, 14/02/2025 17:21).
- **Discovery Source**: The source from which the certificate was discovered (for example, `MicrosoftServer`).
- **Applications Associated**: This column is likely meant to display the applications linked to each certificate, though in the image it appears empty.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Certificate Group**: Indicates the group to which each certificate belongs, set to "Default" in all cases.
- **Certificate Type**: Also set to "Default" for each entry, this column categorizes certificates by their type.

• Click the certificate link to redirect to the Server certificate holistic view.

Bulk Update CSR

1. Go to **Insights** > **Entrust Migration** > **CA Switch Summary**.
2. Select the checkbox for the certificates that you want to update the CSR parameters.
3. Click the **Bulk Update CSR** button.

   The **Update Connector Details** page is displayed to update the CSR parameters.

   Field descriptions for the CA Switch parameters.

Fields	Description
Attachments	
Name	Enter the alternate name for the field to be uploaded.
Comments	Enter the additional information if required.
Upload File	Click the **Upload** button to attach the file.
Certificate Attributes	
Expiry Alert	**Default**: True The Expiry Alert feature notifies users in advance of upcoming certificate expiration dates. This feature helps ensure that certificates are renewed or replaced before they expire, preventing potential service disruptions or security vulnerabilities.
AzureSSOAlertRecipients	The **AzureSSOAlertRecipients** feature refers to a setting or configuration within an Azure environment where specific individuals or groups are designated to receive alerts related to Azure Single Sign-On (SSO) activities.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Vendor specific details	
Certificate Validation Type	**Default**: Email. The dropdown menu under this section shows "Email" as the selected validation type. The available options are: • **Email**: This indicates that email validation will be used for the certificates during the migration process. • **DNS**: his indicates that DNS validation will be used for the certificates during the migration process. **Note:** This field appears only if the **Amazon**, , CA selected in the target CA dropdown list.
Certificate Transparency Logging Preference	**Default**: ENABLED. Select the preference from the dropdown list. The preference for Certificate Transparency Logging is set to **ENABLED**, meaning that the certificates will be logged in publicly accessible Certificate Transparency logs. Available options are: • **ENABLED** • **DISABLED.**

Google 90 Day Dashboard

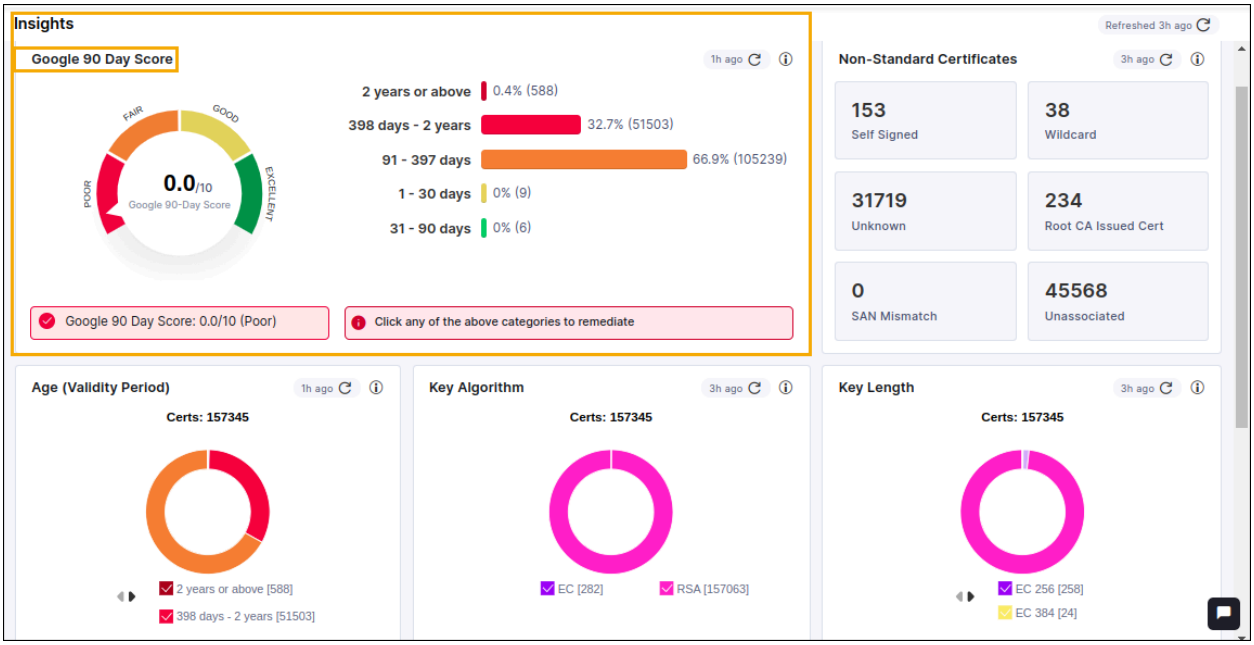
Overview

The Google 90-day certificate refers to Secure Sockets Layer (SSL) certificates issued by Certificate Authorities (CAs) in accordance with Google's guidelines on certificate validity periods. Certificates exceeding 398 days (approximately one year and one month) are considered insecure by Google. This

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

policy encourages the adoption of shorter-lived SSL certificates, typically lasting 90 days, to enhance security and promote timely certificate renewal.

This dashboard displays the reports related to certificate scores, server certificate age, issuers, key algorithms, and key lengths, adhering to the guidelines set by Google for 90-day SSL certificates.



Benefits of Google 90 Day

- **Achieve Visibility**: Clear insight into certificates is crucial for effectively managing renewals and removals. Regular scanning aids in identifying existing certificates and uncovering new ones.
- **Monitor Expiry Dates**: Automation streamlines tracking and upkeep of certificate renewals by issuing timely alerts to relevant personnel. It also ensures proper provisioning and configuration of certificates, along with accurate binding to endpoints.
- **Enforce Encryption Standards**: Encryption forms the cornerstone of certificates, making it imperative to determine the appropriate encryption level to uphold infrastructure security. Analyzing certificates for indicators like key size, strength, or signing algorithms helps identify those utilizing insecure or outdated cryptographic standards.
- **Establish Governance**: While automation aids certificate management, it necessitates a foundational policy for enforcing Public Key Infrastructure (PKI) governance. This governance framework oversees data protection, user identity provisioning, and the security of end-to-end communications.
- **Secure Key Management**: Private keys serve as the ultimate safeguard for sensitive data, yet storing them in unprotected text files exposes them to exploitation. Utilizing encrypted software vaults or certified Hardware Security Modules (HSMs) offers superior protection, particularly if automated key rotation is enabled to periodically replace them.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

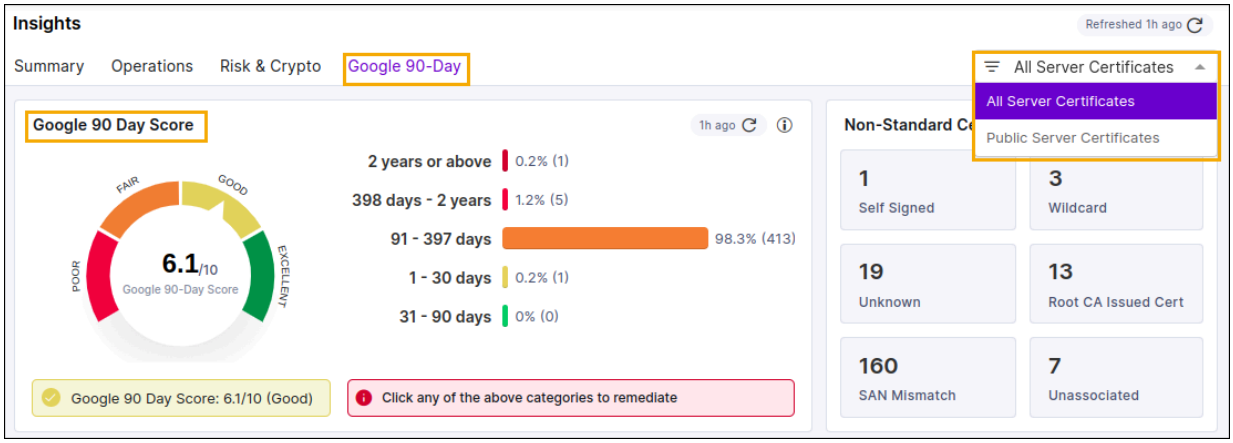
Showing Report For

The Google 90-day dashboard showcases two types of reports along with specific widgets:

- **All Server Certificates**: All Server Certificates refers to a category or group that includes all types of server certificates, regardless of their specific characteristics or attributes.

> **Note:** To access the report for the entire system, users must belong to the admin group with super access.

- **Public Server Certificates**: Certificates that have a trust chain consisting of a public root certificate and intermediate certificates are categorized as public certificates.



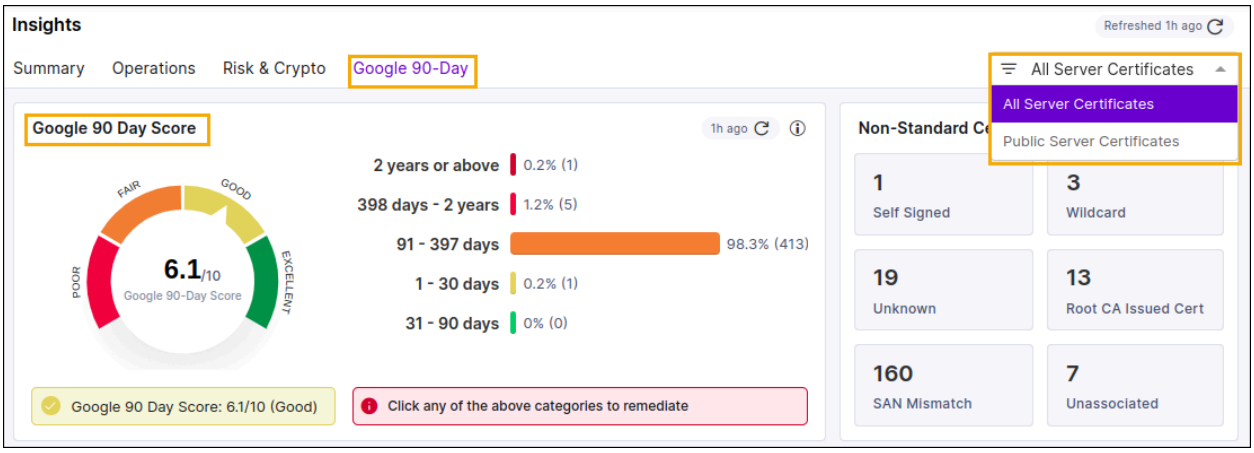
Google 90 Day Score

This report displays the score of certificate based on the certificate age and certificate count categorization on the single certificate validation time.

Certificate Age: This report presents the severity status of certificates. A certificate includes a created date and an expiry date, and the number of days between these dates is referred to as the certificate age. The terms Validity Period and Certificate Age share the same definition. Following are the status based on age limit:

- 2 years or above - CRITICAL
- 398 days - 2 years - HIGH
- 91 - 397 days - MEDIUM
- 1 - 30 days - LOW.
- 31 - 90 days - Good.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

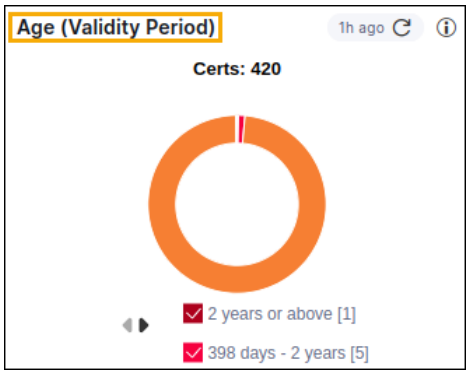


Certificates Count: The certificate count report displays the number of non-standard certificates. You can click on the count, which will redirect to the server certificate inventory.

Age (Validity Period)

The server certificates are grouped by validity in the Age (Validity Period) report, displays the different validity periods as shown on the image. The pie chart's colored sections represent the count and validity status of the certificates. You have the following options:

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.

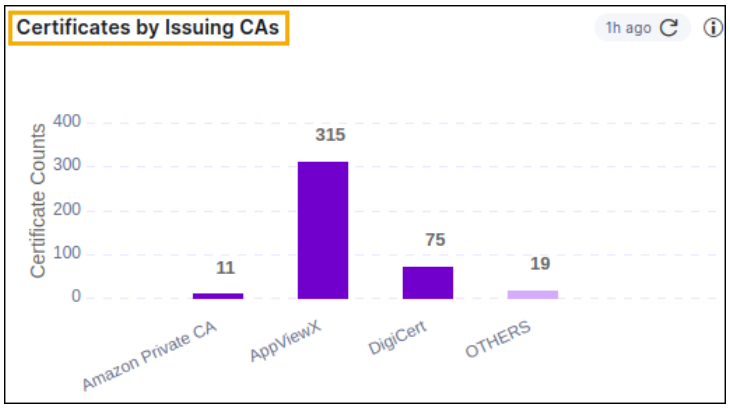


By Issuers

The server certificates are categorized by issuing vendors. The By Issuers report displays all the server certificates that are currently managed or monitored, excluding expired and revoked. You have the following options:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

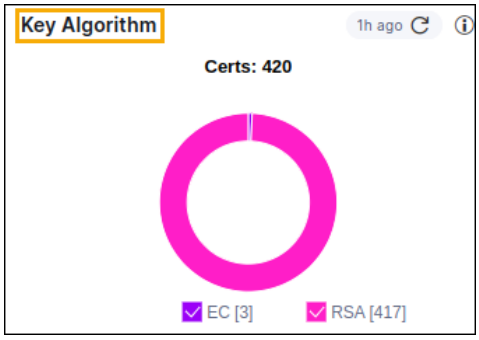
- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.



Key Algorithm

This report displays the count of server certificates by key algorithm. Different colored sections of the pie chart represent the count of server certificates based on the key algorithm. For instance, RSA (59), DSA (10), and so on. You have the following options:

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.

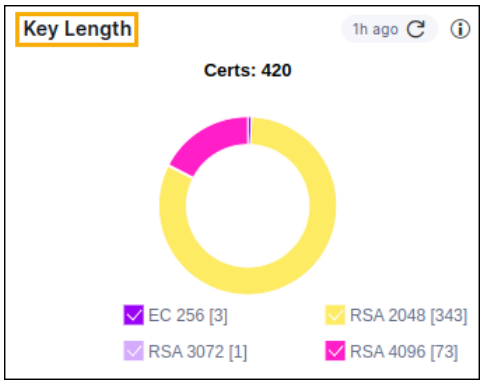


Key Length

This report displays the count of server certificates by key length. Different colored sections of the pie chart represent the count of server certificates based on the key length. For instance, RSA (59), DSA (10), and so on. You have the following options:

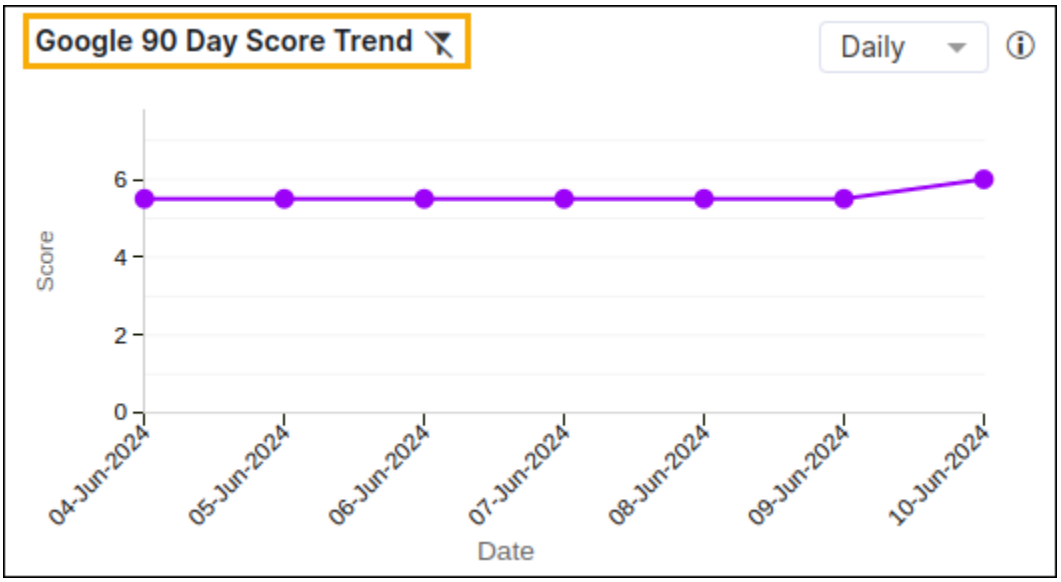
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Select the check-box to view the specific portion, excluding unselected items.
- Click on the pie chart to redirect to the server certificate inventory.



Google 90 Day Score Trend

Stated in the Google 90-day standard proposal, certificates are grouped based on their validity, and a score is calculated for each certificate. These scores are then aggregated to generate the Google 90-day score.



Non-Standard Certificates

Displays a report detailing the count of non-standard certificates in the following categories:

- Self-Signed
- Wildcard
- Unknown
- Root CA Issued Certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

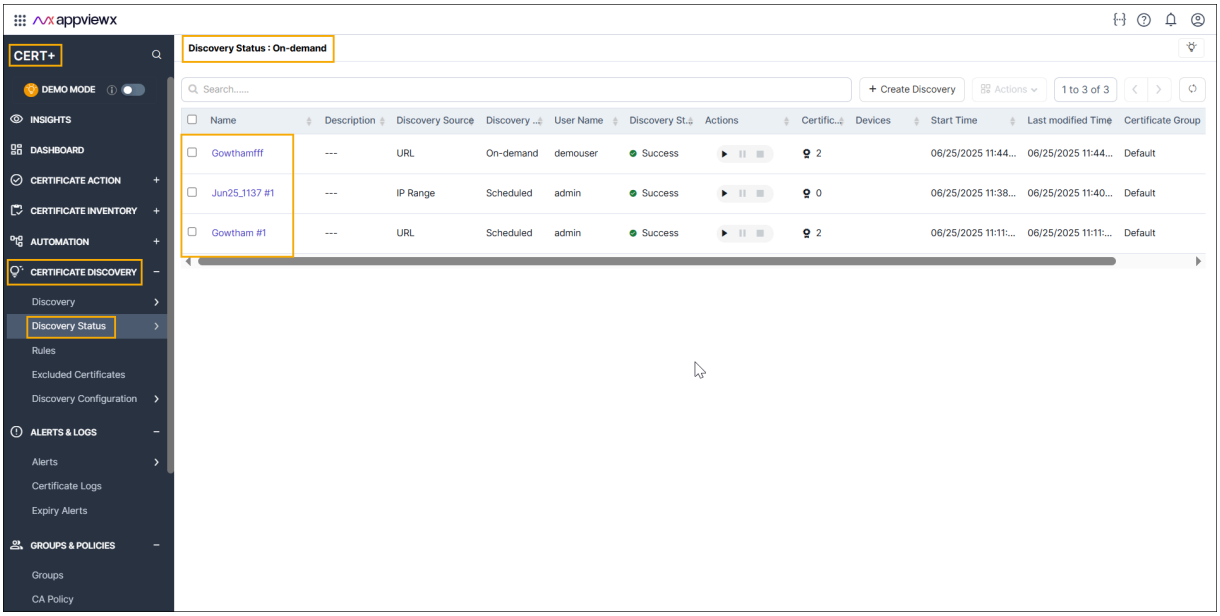
- SAN Mismatch
- Unassociated Certificates.

Threshold Limits

- For less than 100,000 certificates, live data will be displayed whenever the user navigates to the Insights page.
- For more than 100,000 certificates, a pre-calculated report will be shown with the last generated time indicated at the widget level.
- Users can click the widget level refresh to view the live data.

Accessing the Discovery Summary Dashboard

1. Go to (**Menu**) > **CERT+** > **Dashboard**.
   The dashboard home page is displayed.
2. To go to the Discovery Dashboard, from the top left corner of the screen, click Discovery URL.
   The **Dashboard** summary page is displayed.



- Understanding the Discovery Certificate Dashboard

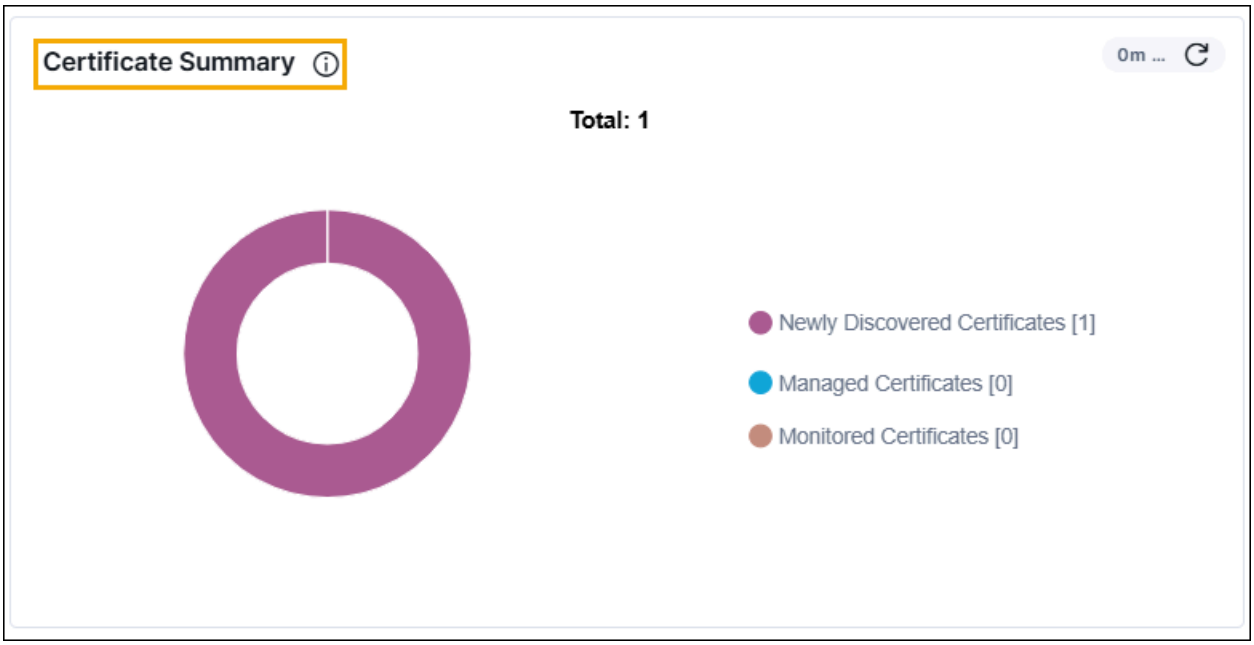
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Understanding the Discovery Certificate Dashboard

This dashboard displays reports related to the certificates from the certificate discovery. You can access this dashboard from the **Discovery Status** CERTIFICATE DISCOVERY page, by selecting **On Demand** option.

Certificate Summary

This widget provides a quick snapshot of the overall certificate landscape, highlighting the influx of new certificates and the proportion under active management or monitoring. A high number of newly discovered certificates may warrant further investigation.

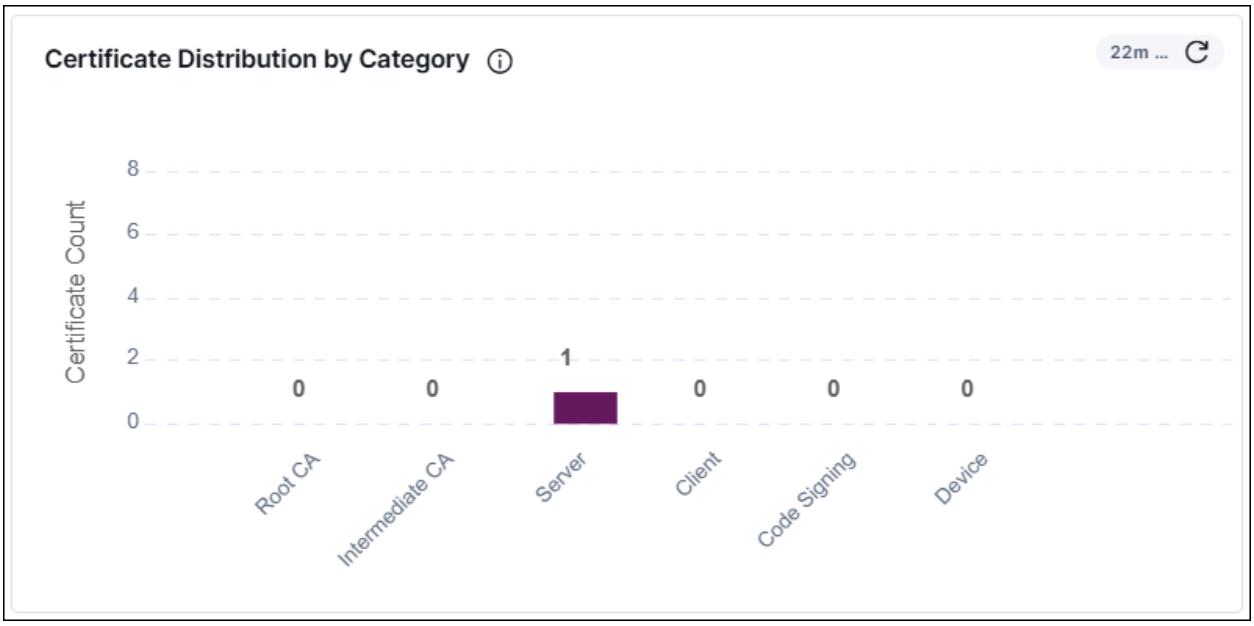


Certificate Distribution by Category

This widget helps you understand the distribution of certificate types, identifying their primary use within your environment and highlighting areas that may need focused management or stronger security policies. For example, a high number of server certificates may suggest a large web infrastructure.

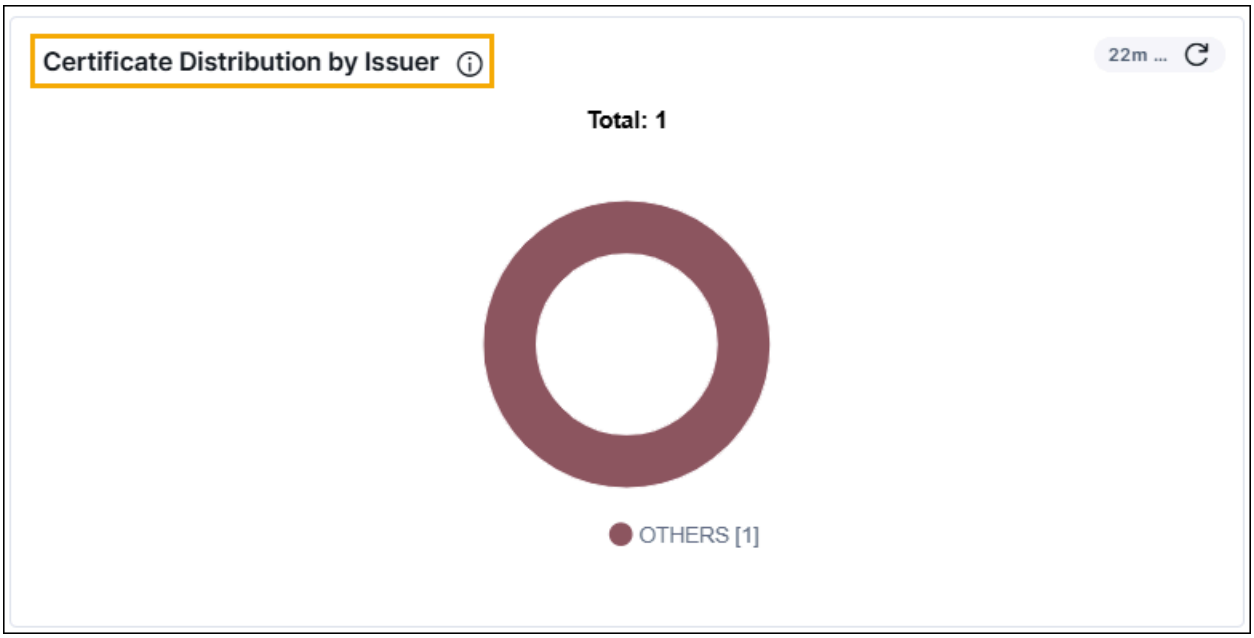
.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Certificate Distribution by Issuer

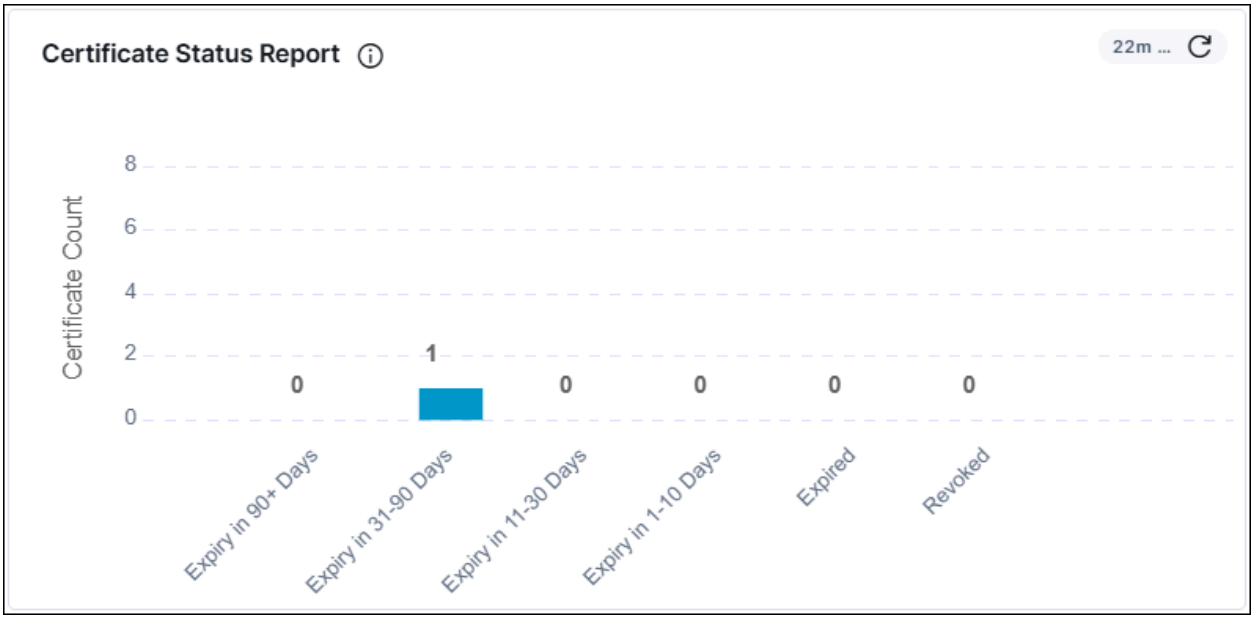
This widget provides insight into which entities issued your certificates—crucial for trust management and understanding dependencies on various certificate authorities. If specific issuers are identified, the chart visualizes the proportion of certificates issued by each. The current view indicates a need to investigate the issuers for improved visibility.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Status Report

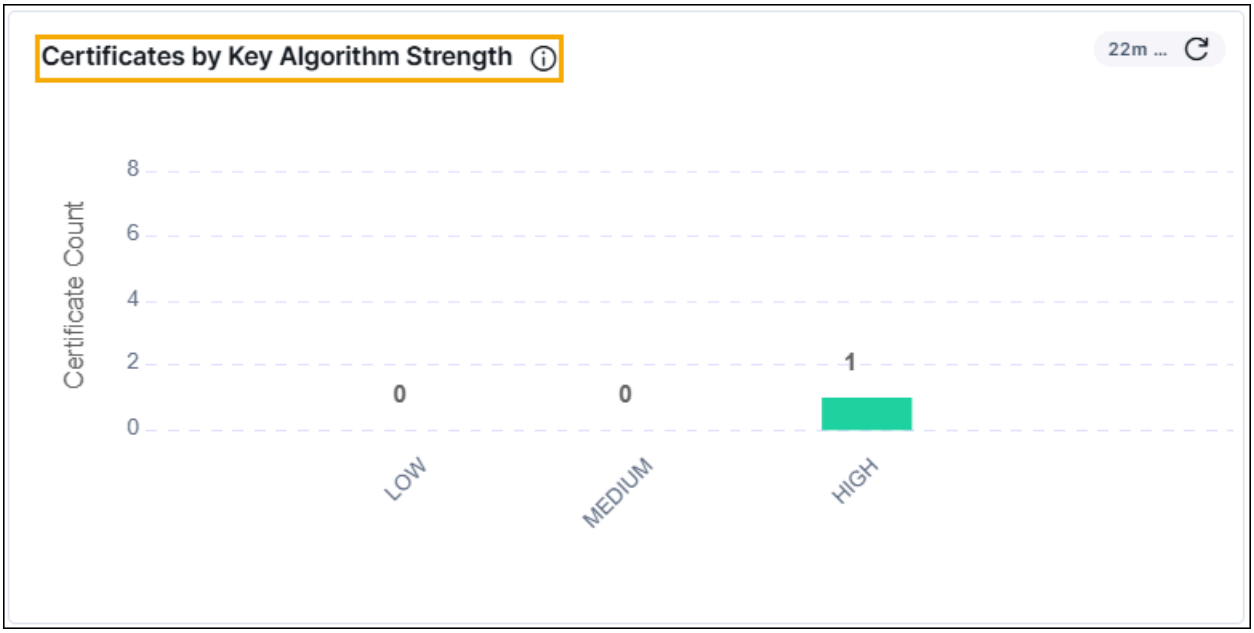
This widget is essential for proactive certificate management, helping you quickly identify certificates that are nearing expiry or already expired. It supports timely renewals to prevent service disruptions and security risks. Additionally, the count of revoked certificates may indicate potential security incidents or policy enforcement actions.



Certificates by Key Algorithm Strength

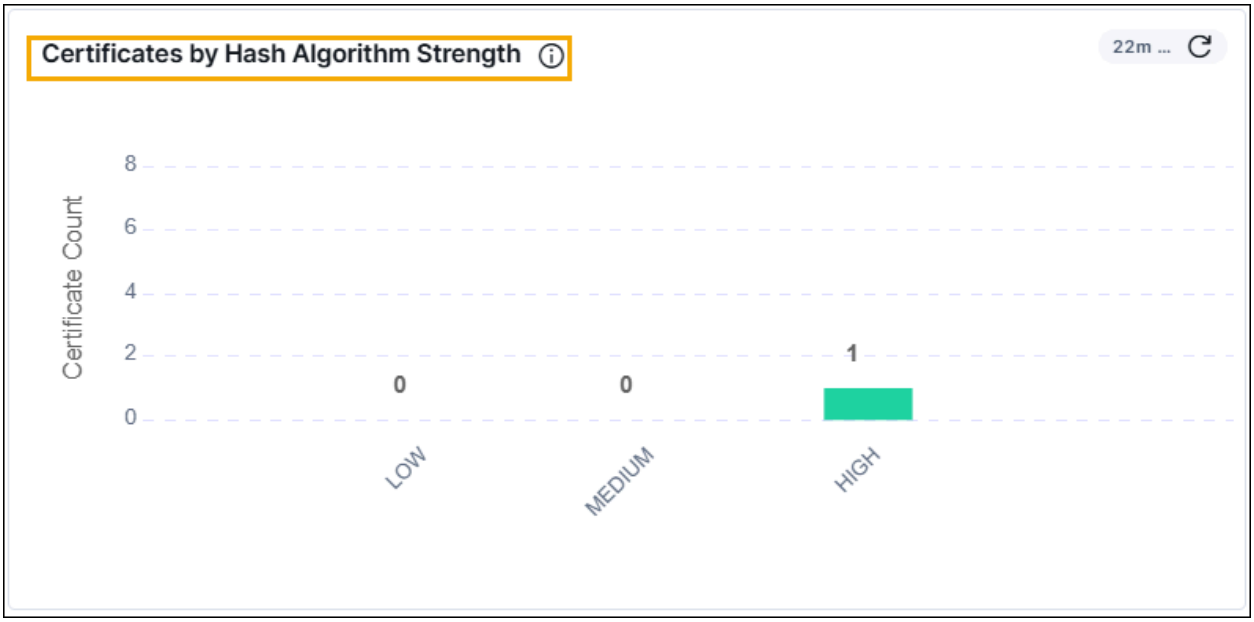
This widget helps assess the cryptographic strength of your certificates, offering insight into your overall security posture. A high number of certificates using low or medium strength algorithms may signal potential vulnerabilities and the need to upgrade to stronger algorithms. Ideally, most certificates should fall into the 'High' strength category.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Certificates by Hash Algorithm Strength

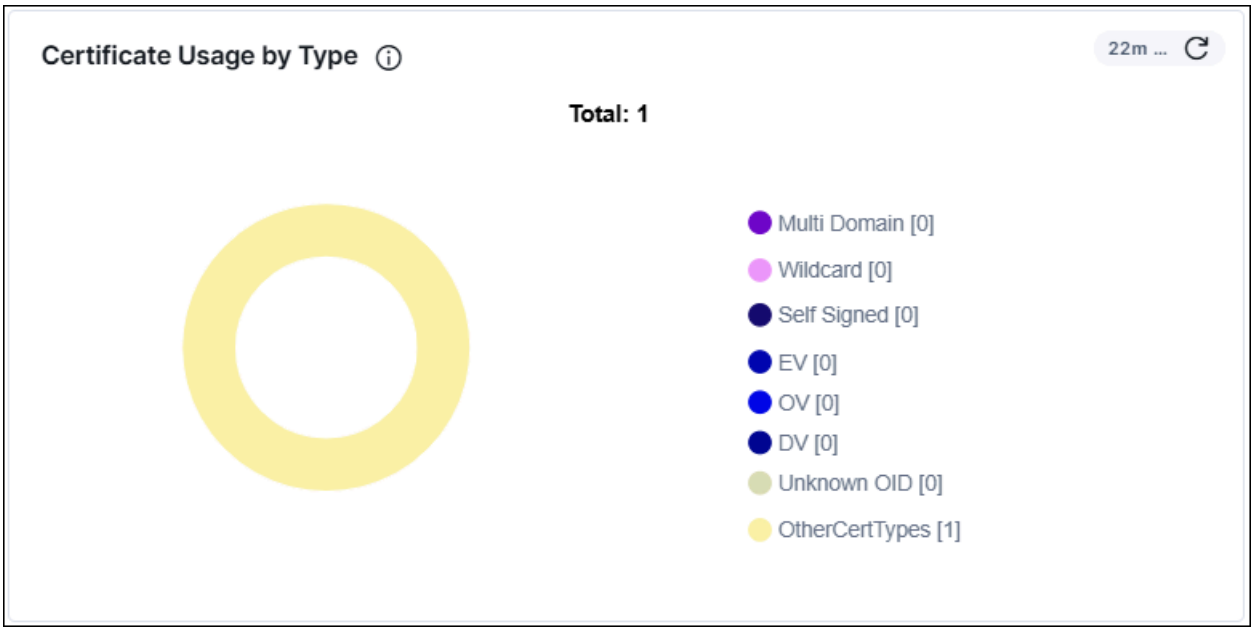
The hash algorithm ensures certificate integrity. Certificates using weak hash algorithms pose a security risk, as they can be more easily tampered with. This widget helps identify such certificates and prioritize their migration to stronger, more secure algorithms.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Type Distribution

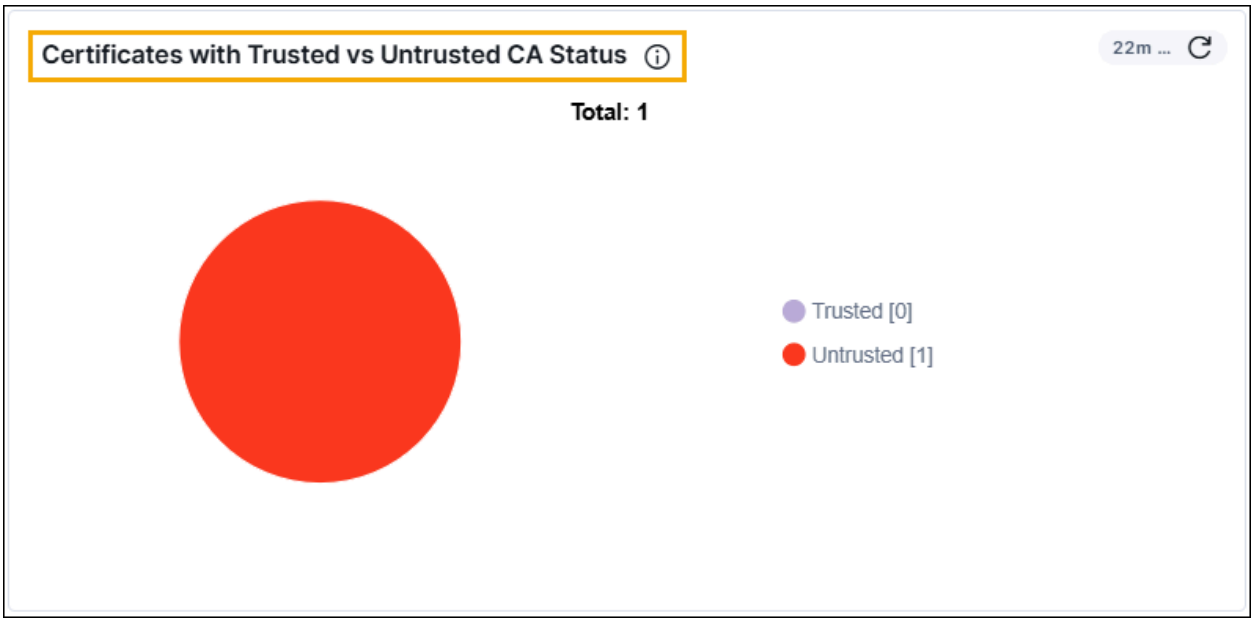
This widget helps understand dependency on various device or server vendors. This insight is valuable for vendor management, cost analysis, and aligning with organizational policies on infrastructure diversity or consolidation. It can also highlight potential single points of failure associated with specific vendors.



Certificates with Trusted vs Untrusted CA Status

This widget is crucial for assessing the trustworthiness and security of the certificate ecosystem. Ideally, the vast majority of certificates should be issued by trusted CAs. A high number of untrusted certificates may indicate security risks, misconfigurations, or the use of self-signed certificates where CA-signed ones are recommended. Investigating and addressing untrusted certificates is essential for maintaining a secure environment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



PQC Compliance Certificates

This widget highlights readiness for the post-quantum era, as current cryptographic algorithms may become vulnerable with advances in quantum computing. A high number of non-compliant certificates signals a potential future security risk, making long-term planning for migration to PQC-compliant algorithms essential. At present, with all certificates marked as non-compliant, this represents a key area to monitor and prepare for as PQC standards and implementations evolve.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Alerts and Logs

- Overview
- Certificate Alerts
- Configuring Expiry Alerts
- Configuring a Certificate Expiry Alert
- Configuring a Certificate Sync Alert
- Configuring a Certificate Validation Alert
- Configuring a Connection Failure Alert
- Configuring a CLM Action Failure Alert
- Certificate Logs
- Export Certificates Logs

Overview

CERT+ allows you to monitor the AppViewX component level and certificate-related alerts in a dashboard with predefined filters. Also, you can configure alerts based on your business needs. With these alerts, you can trigger an email with the necessary information. To run a custom logic based on the alert condition, you can configure it through a visual workflow in AppViewX. Alerts and logs help you to ensure the system performance is monitored.

You can view logs and receive certificate alerts through,

- Certificate Logs
- Certificate Alerts

Certificate Alerts

Certificate Alerts helps you with alerts that are related to certificates. You can configure these alerts based on certificate events such as sync, validation, or expiry. Any certificate-related actions performed in your application are captured as logs. Also, you can notify users of a specific certificate action through these alerts.

To verify certificate alerts,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

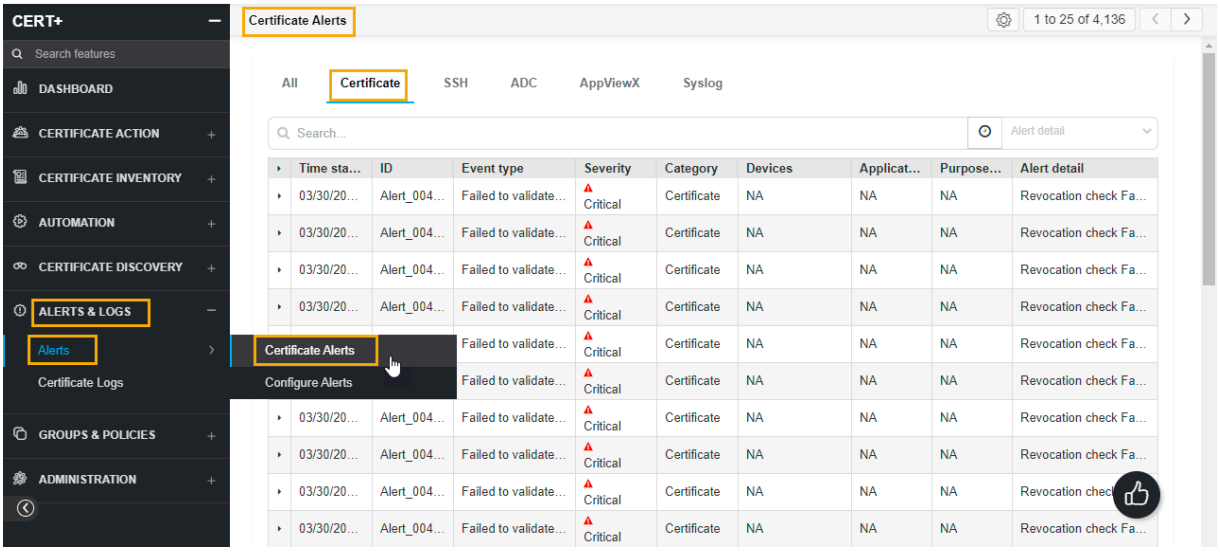
The left navigation pane appears.

3. Click **CERT+**.

   The **CERT+** left navigation pane appears.

4. Expand **ALERTS & LOGS**.
5. Click **Alerts**, and then select **Certificate Alerts**.

   The **Certificate Alerts** screen appears.



6. On the Certificate Alerts list view page, you can find the list of alerts related to the certificates. Any actions performed on the certificates are captured under this list view.
7. You can search for alerts based on the Alert ID, Alert Event type, Severity, Category, Devices, Applications, and Alert detail.
8. On the alert screen, view all details for a log by hovering your cursor over each column of data or click the (Expand) icon for the log you want to view. The table row expands to display all details for the log.

Configuring Expiry Alerts

Digital certificates are issued with a validity period predefined by the certificate authorities. When a certificate outgrows this validity period, it is no longer trusted and the services consuming the certificate are considered broken.

AppViewX lets you create certificate expiry alerts, which are proactive notifications to customers to renew the certificates that are due for expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The alerts are primarily created based on the period of certificate expiry (certificates expiring on a specific date, certificates expiring after x number of days, and so on). The emails also include a certificate renewal link, thus simplifying the CLM process.

The following sections list the prerequisites for configuring the expiry alerts and the configuration steps.

- Configuring Certificate Expiry Alerts over Email
- Configuring Certificate Expiry Alerts over ITSM
- Configuring Certificate Expiry Alerts using Custom Workflows
- Placeholders for Retrieving Certificate Details
- Disabling Expiry Alerts Manually

Configuring Certificate Expiry Alerts over Email

Before configuring certificate expiry alerts over emails, **ensure that permissions to create and modify the expiry alerts are assigned to the required role(s)**.

Note: Certificate renewal is allowed only for users having read and write permission to the certificate group. Ensure that you assign permissions accordingly.

1. To do this, follow the instructions given here and enable **Expiry Alerts** under **Authorized Functions** > **CERT+**.
2. Modify the resource mapped to this role to assign the following workflow requests (**Access Control** > **Workflow Requests**) to the resource:
   - **Cert_Expiry_Mail_Individual**
   - **Cert_Expiry_Mail_Bulk**

To configure certificate expiry alerts over email:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Expiry Alerts**.
   The expiry alerts inventory is displayed.
2. To create a new email expiry alert, click **+ Create**.
   The **Expiry Alert > Expiry Alert Add** page is displayed.

Tip: This page has a list of best practices you are advised to follow when creating a new expiry alert.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. For the new alert, enter a unique **Alert Name** (mandatory) and a description (optional) with additional details about the alert.
4. In the **Alert Configuration** section, click **+ Add**.
   The **Add Configuration** pane is displayed.
5. Select the **Certificate Type** for which you want to configure the expiry alert.
   - **End Certificate**
   - **CA Certificate**
6. Enter the **Filter Configuration** details.

Field descriptions for the Filter Configuration section

Field	Description
Certificate Expiry Period	To filter certificates based on their expiry: • **Range in days**: Sends an expiry alert email for certificates that will expire within the specified range of days from the current date For example, to set an alert for certificates that will expire between 10 and 40 days from the current calendar date, enter **10** and **40**. Alerts will be sent for all certificates expiring between 00:00:00 AM on the start day and 11:59:59 on the end day. • **On specified days**: Sends an expiry alert email for certificates that will expire on the nth day from the current date For example, to send an alert for certificates expiring on the 50th day from the current calendar date, enter **50**. Alerts will be sent for all certificates expiring between 00:00:00 AM and 11:59:59 PM of the specified day. • **Range in dates**: Sends an expiry alert email for all certificates expiring in a specific duration Use the calendar widget to select the **Start date** and **End date** for this duration. Alerts will be sent for all certificates expiring between 00:00:00 AM on the start date and 11:59:59 on the end date.
Additional Filters	To add a filter in addition to the certificate expiry period: a. Select the required filter from the **Select option** dropdown list. b. Enter the corresponding value in the **Type to enter value** field. c. Click **Add**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected filter option and its value are displayed.
***Notification Method**	To send an expiry alert over email, select **Email**. **Note:** For instructions on sending an expiry alert over an ITSM tool (ServiceNow/JIRA), click here.
Individual Alerts : Allow certificate renewal	This field is displayed only when **Notification Method** = **Email**. To trigger individual emails for each certificate that matches the filter criteria along with a renewal and unsubscribe link for the certificate, enable this button.
Ignore renewed/ regenerate certificate	To stop alerts for certificates that have already been renewed or regenerated, enable this button.
Ignore Alerts if No Certificate Expirations	By default, this is enabled. Disabling this option will trigger alerts even if there are no certificate expirations to report.

7. Enter the **Email Configuration** details.

Field descriptions for the Email Configuration section

Field	Description
Template	From the dropdown list, according to the format and structure of the email content required, select an email template. This dropdown list is populated with predefined email templates that can be created and managed in the **Platform** module of the product. For instructions on creating a custom email template, click here.
To*	
Recipient(s)	Enter the recipient(s) email address. You can enter a maximum of 20 email addresses separated by a comma.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Parameter(s)	To add more recipients for the alert email, you can retrieve email addresses from the following certificate parameters: • Subject Email • SAN (rfc822) • Certificate Group From the dropdown list, select the required parameter(s).
Certificate Attribute(s)	To add more recipients for the alert email, you can retrieve email addresses from any certificate attribute that has the email ID as its value, for example, **Cert Owner**. From the dropdown list, select the certificate attribute.
CC	
Recipient(s)*	Enter the email address of stakeholders who are to receive a copy of the expiry alert email.
Certificate Parameter(s)	To add more recipients to the CC field in the alert email, you can retrieve email addresses from the following certificate parameters: • Subject Email • SAN (rfc822) • Certificate Group From the dropdown list, select the required parameter(s).
Certificate Attribute(s)	To add more recipients to the CC field in the alert email, you can retrieve email addresses from any certificate attribute that has the email ID as its value, for example, **Cert Owner**. From the dropdown list, select the certificate attribute.
Email Subject	
Subject*	Enter the subject line for the expiry alert email using the following (recommended) format: **Expiry Alert :: |Common Name| certificate| expiring on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Body*	Enter the body text for the email using the following (recommended) format:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Certificate with Common Name |Common Name| **Serial number |Serial Number|** **issued by |Issuer Common Name|** **is about to expire on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.

8. Click **Add**.

   The created alert is listed in the table below the **+ Create** button.

   Tip: To edit/delete an alert, use the **Edit**/**Delete** button, as required.

9. Under **Alert Execution Type**:

   Note: The settings configured here will be applicable to all expiry alerts listed in the above table.

   a. To configure a manual alert that will be triggered immediately, select **Run Now** and click **Save**.

      Note: Once an alert has been created, it's execution type cannot be modified.

   OR

   a. To trigger the alert at a scheduled time, select **Schedule** and enter the following details:
      - **Time Zone***
      - **Frequency** (daily/weekly/monthly/yearly)
      - **Starts On***
      - **Ends**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- For ends **ON**, use the calendar widget to select the date on which the last expiry alert email will be sent.
- For ends **After**, enter the number of **Occurrences** after which the expiry alert will be discontinued.

10. Click **Save**.

    Once the expiry alerts are configured with **Allow certificate renewal option**, the individual certificate renewal email will be sent to the stakeholders with two links:

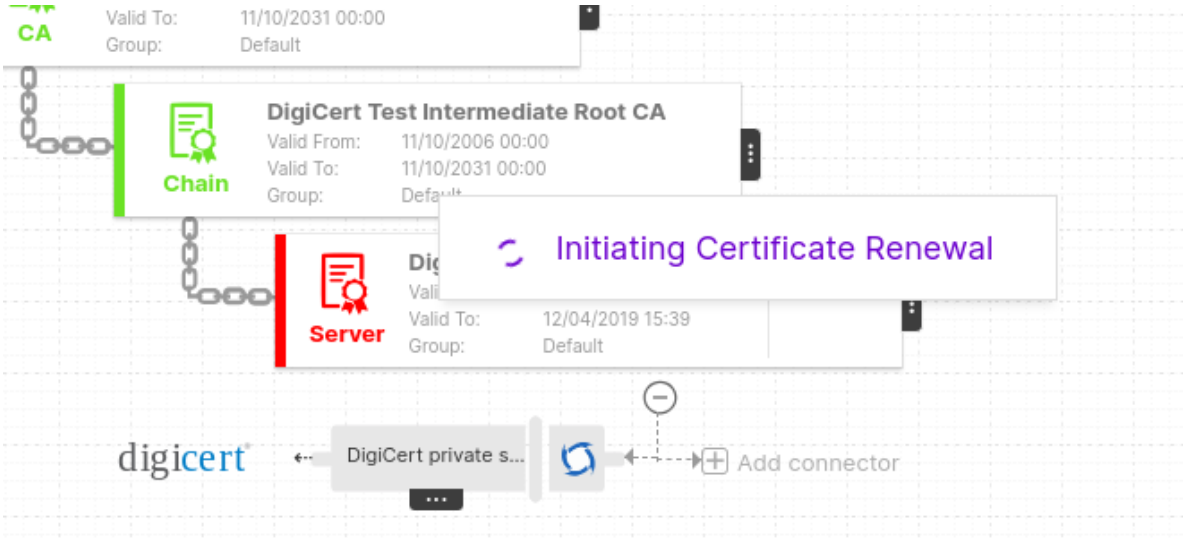
    - Link for certificate renewal
    - Link for unsubscribing from the alerts for that specific certificate

> **Tip:** You can repeat steps **4** to **9** to add more than one **Alert Configuration** under a **Alert Name**.

11. To renew the certificate:

    a. Click the renewal link and login to AppViewX.

    You will be redirected to the holistic view for the certificate and the following renewal alert will be displayed:

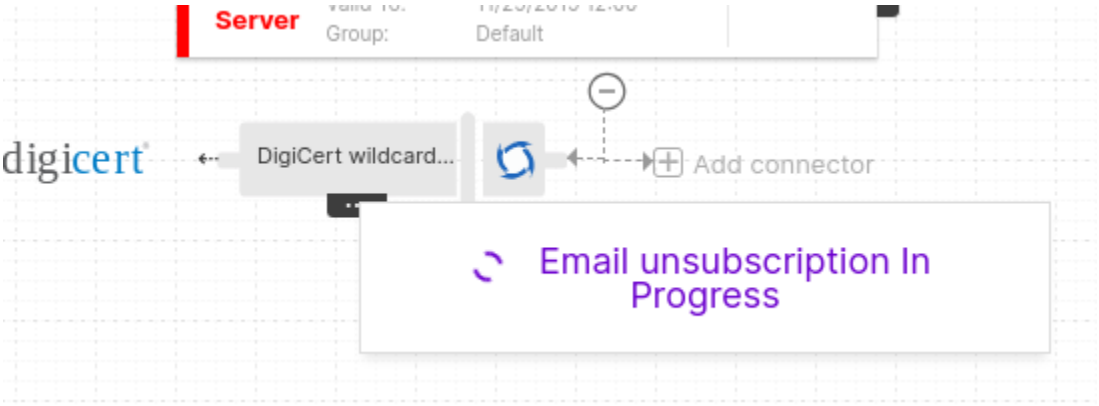


    b. For instructions on how to renew a certificate, refer to the documentation for renewing a certificate.

To unsubscribe from the alerts for the certificate, click the unsubscribe link from the alert email.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

You will be redirected to the certificate inventory page and the following unsubscribe alert will be displayed:



• Use Cases for Configuring Expiry Alerts

Use Cases for Configuring Expiry Alerts

Use Case 1

Objective: Application owners want to configure alerts specific to their application.

Alert Criteria 1: Bulk notification

Alert Criteria 2: Individual certificate notification (recommended)

Configuring an Expiry Alert for Alert Criteria 1

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert criteria 1 configuration

Alert parameter	Value
Range in days	20 - 30
Filter	Certificate group < select the application group>
Notification Format	Attachment
To	< Recipient as application group email ID > Certificate group : <select the application group>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Alert parameter	Value
CC	<admin group email id>
Subject	Expiry Alert :: Certificates expiring in next 30 days
Body	Common Name, Serial Number, Valid From , Valid Until

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert criteria 1 configuration

Alert parameter	Value
Range in days	0 - 10
Subject	Expiry Alert :: Certificates Expiring in 10 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Configuring an Expiry Alert for Alert Criteria 2

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert criteria 2 configuration

Alert parameter	Value
Range in days	20 - 30
Allow Users Renewal	Enabled
Filter	Certificate group < select the application group>
To	< Recipient as application group email ID > Certificate group : <select the application group>
CC	<admin group email id>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Alert parameter	Value
Subject	Expiry Alert :: |Common Name| certificate is expiring on |Valid Until|
Body	|Common Name| certificate is expiring on |Valid Until| issued by |Issuer Common Name|

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

   Updated values for the alert criteria 2 configuration

Alert parameter	Value
Range in days	0 - 10
Subject	Expiry Alert : Critical : |Common Name| certificate is expiring on | Valid Until|
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Use Case 2

Objective: The PKI team will receive the alerts and take remediation action, following up with the application owners. The PKI team will get a list of certificates expiring on the 30th day from the day of alert configuration and must then consult with the application owners. Reminders for certificates missing from remediation for 20 days should be part of a critical alert condition.

Alert Criteria 1: Bulk notification (recommended)

Alert Criteria 2: Individual certificate notification

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring an Expiry Alert for Alert Criteria 1

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert criteria 1 configuration

Alert parameter	Value
On specified days	30
Filter	Certificate group < select the application group>
Notification format	Attachment
To	< PKI Admin > Certificate group : <select the application group>
CC	<Certificate group>
Subject	Expiry Alert :: Certificates expiring in next 30 days
Body	Common Name, Serial Number, Valid from , Valid Until, Issuer Common Name

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert criteria 1 configuration

Alert parameter	Value
On specified days	10
Subject	Expiry Alert :: Certificates Expiring in 10 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring an Expiry Alert for Alert Criteria 2

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert criteria 2 configuration

Alert parameter	Value
On specified days	30
Allow Users Renewal	Enabled
Filter	Certificate group < select the application group>
To	< Recipient PKI Admin > Certificate group : <select the application group>
CC	<Certificate group>
Subject	Expiry Alert :: |Common Name| certificate is expiring on |Valid Until| for the group |Certificate Group|
Body	|Common Name| certificate is expiring on |Valid Until| issued by |Issuer Common Name|

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Updated values for the alert criteria 2 configuration

Alert parameter	Value
On specified days	10
Subject	Expiry Alert : Critical : |Common Name| certificate is expiring on |Valid Until| for the group | Certificate Group Name|
Alert execution type	Scheduled; everyday from the day of alert configuration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Use Case 3

Objective: The administrator wants to send expiry alerts for certificates expiring in the next 30 days to all the application owners (who will take remedial action on their respective certificates). The administrator also wants to send a critical reminder to the application owners if an action has not been taken in the next 15 days.

Alert Criteria 1: Bulk notification

Alert Criteria 2: Individual certificate notification

Configuring an Expiry Alert for Alert Criteria 1

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert criteria 1 configuration

Alert parameter	Value
Range in days	0 - 30
Allow user Renewal	Enabled
To	Certificate group : <select the application group>
CC	<admin group email id>
Subject	Expiry Alert :: |Common Name| certificate is expiring on |Valid Until|
Body	|Common Name| certificate is expiring on |Valid Until| issued by |Issuer Common Name|
Alert execution type	Scheduled; everyday from the day of alert configuration

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Updated values for the alert criteria 1 configuration

Alert parameter	Value
Range in days	0 - 15
Subject	Expiry Alert :: Certificates not taken action for past 15 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration; ends after 15 days

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Configuring an Expiry Alert for Alert Criteria 2

1. Create an expiry alert using the alert configuration given in the table below.

Values for the alert criteria 2 configuration

Alert parameter	Value
Range in days	0 - 30
Notification Format	Attachment
To	Certificate group : <select the application group>
CC	<admin group email id>
Subject	Expiry Alert :: Certificates expiring in next 30 days
Body	Common Name, Serial Number, Valid From , Valid Until, Issuer Common Name
Alert execution type	Scheduled; everyday from the day of alert configuration; ends after 15 days

2. Click **Add**.
   The alert is added to the table in the **Alert Configuration** section.
3. Under **Alert Configuration**, click **Add**.
4. Use the alert parameters and values given in step 1 and only edit the parameters given in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Updated values for the alert critera 2 configuration

Alert parameter	Value
Range in days	0 - 15
Subject	Expiry Alert :: Certificates not taken action for past 15 days :: Critical
Alert execution type	Scheduled; everyday from the day of alert configuration; ends after 15 days

5. Click **Add**.
   The updated alert is also added to the table in the **Alert Configuration** section.

Configuring Certificate Expiry Alerts over ITSM

Prerequisites

Ensure that the ITSM tool you want to receive alerts on is integrated with AppViewX via tha Integration Hub. For instructions, you can refer to the documentation here.

Configuring Expiry Alerts over ITSM

Important: Expiry alerts over email can be configured for end certificates as well as CA certificates. Expiry alerts over ITSM channels can be configured only for end certificates.

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Expiry Alerts**.
   The expiry alerts inventory is displayed.
2. To create a new ITSM expiry alert, click **+ Create**.
   The **Expiry Alert > Expiry Alert Add** page is displayed.

   Tip: This page has a list of best practices you are advised to follow when creating a new expiry alert.

3. For the new alert, enter a unique **Alert Name** (mandatory) and a description (optional) with additional details about the alert.
4. In the **Alert Configuration** section, click **+ Add**.
   The **Add Configuration** pane is displayed.
5. From the **Certificate Type** field, select **End Certificate**.
6. Enter the **Filter Configuration** details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Filter Configuration section

Field	Description
Certificate Expiry Period	To filter certificates based on their expiry: • **Range in days**: Sends an expiry alert email for certificates that will expire within the specified range of days from the current date For example, to set an alert for certificates that will expire between 10 and 40 days from the current calendar date, enter **10** and **40**. Alerts will be sent for all certificates expiring between 00:00:00 AM on the start day and 11:59:59 on the end day. • **On specified days**: Sends an expiry alert email for certificates that will expire on the nth day from the current date For example, to send an alert for certificates expiring on the 50th day from the current calendar date, enter **50**. Alerts will be sent for all certificates expiring between 00:00:00 AM and 11:59:59 PM of the specified day. • **Range in dates**: Sends an expiry alert email for all certificates expiring in a specific duration Use the calendar widget to select the **Start date** and **End date** for this duration. Alerts will be sent for all certificates expiring between 00:00:00 AM on the start date and 11:59:59 on the end date.
Additional Filters	To add a filter in addition to the certificate expiry period: a. Select the required filter from the **Select option** dropdown list. b. Enter the corresponding value in the **Type to enter value** field. c. Click **Add**. The selected filter option and its value are displayed.
Notification Method	To send an expiry alert over ITSM, select **Others**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Ignore renewed/ regenerated certificate	When this field is enabled, results returned after the alert is triggered will not include certificates that have already been renewed or regenerated, even though they match the filter criteria.
***ITSM Tool**	This field is displayed only when **Notification Method** = **Others**.From the following options in the dropdown list, select an ITSM tool to raise a ticket for the alert: • **ServiceNow** • **JIRA**

7. To receive expiry alerts on **ServiceNow**:

   a. From the following options, select the **Configuration Type**:
   - **Basic**: Create a ticket by specifying the minimum details in the **Configuration** section.
   - **Advanced**: Based on the organization policy, fill the required values for a ticket using a JSON. In this case, a JSON editor will replace the **Configuration** section. The JSON is editable and can be customized as per requirement.

   b. From the following options, select the **Issue Type**:
   - **Incident** (Tickets will be listed on the **Incidents** page)
   - **Service Request** (Tickets will be listed on the **My requests** page)

   c. Enter the **Configuration** details.

Field description for Incident requests

Field	Description
Short Description*	Enter a title/short description for the ticket alert using the following (recommended) format: **Expiry Alert :: |Common Name| certificate| expiring on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Description*	Enter a detailed description of the incident event here (for example, certificate details and operation links) using the following (recommended) format:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Certificate with Common Name |Common Name| **Serial number |Serial Number|** **issued by |Issuer Common Name|** **is about to expire on |Valid Until|** The field will retain all line breaks as added. **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Urgency*	From the dropdown list, select the urgency level of the incident.
Impact*	From the dropdown list, select the impact level of the incident.
Assignment Group*	Enter the name of the group this incident will be assigned to.

Field description for Service Requests

Field	Description
Short Description*	Enter a title/short description for the ticket alert using the following (recommended) format: **Expiry Alert :: |Common Name| certificate| expiring on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Description*	Enter a detailed description of the incident event here (for example, certificate details and operation links) using the following (recommended) format: **Certificate with Common Name |Common Name|** **Serial number |Serial Number|**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	issued by |Issuer Common Name| **is about to expire on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Priority*	From the dropdown list, select the priority assigned to the incident.
Assigned to*	Enter the name of the user this incident will be assigned to.
Due Date*	Using the calendar widget, select a due date for the ticket.

d. Click **Validate**.

OR

To receive expiry alerts on **JIRA**:

a. From the following options, select the **Configuration Type**:
- **Basic**: Create a ticket by specifying the minimum details in the **Configuration** section.
- **Advanced**: Based on the organization policy, fill the required values for a ticket using a JSON. In this case, a JSON editor will replace the **Configuration** section. The JSON is editable and can be customized as per requirement.

b. Enter the **Configuration** details.

Field descriptions for the Configuration details

Field	Description
Project Id*	Enter the unique identifier of the project in JIRA under which the JIRA ticket will be created. **Note:** For instructions on how you can find the JIRA project ID, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Issue Type*	From the dropdown list, select the type of JIRA issue.
Summary*	Enter a title/short description for the JIRA ticket using the following (recommended) format: **Expiry Alert :: |Common Name| certificate| expiring on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Description	Enter additional details related to the ticket using the following (recommended) format: **Certificate with Common Name |Common Name|** **Serial number |Serial Number|** **issued by |Issuer Common Name|** **is about to expire on |Valid Until|** **Note:** • Specify the dates in the mm/dd/yyyy format. • The full list of placeholders and their corresponding values is given here.
Priority*	From the dropdown list, assign a priority to the ticket.
Reporter	Enter the name of the user who reported the issue. **Important:** For the JIRA server, only the AD user name (in the format **name.lastname**) is the accepted value for this field. Email ID or user name are **invalid** values.
Assignee*	Enter the name of the user to whom this JIRA ticket will be assigned.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: For the JIRA server, only the AD user name (in the format **name.lastname**) is the accepted value for this field. Email ID or user name are **invalid** values.

c. Click **Validate**.

8. Click **Add**.
   The created alert is listed in the table below the **+ Create** button.

> **Tip:** To edit/delete an alert, use the **Edit**/**Delete** button, as required.

9. Under **Alert Execution Type**:

> **Note:** The settings configured here will be applicable to all expiry alerts listed in the above table.

a. To configure a manual alert that will be triggered immediately, select **Run Now** and click **Save**.

OR

a. To trigger the alert at a scheduled time, select **Schedule** and enter the following details:
   - **Time Zone***
   - **Frequency** (daily/weekly/monthly/yearly)
   - **Starts On***
   - **Ends**
     - For ends **ON**, use the calendar widget to select the date on which the last expiry alert email will be sent.
     - For ends **After**, enter the number of **Occurrences** after which the expiry alert will be discontinued.

> **Note:** Once an alert has been created, it's execution type cannot be modified.

10. Click **Save**.
    Once the expiry alerts are configured with **Allow certificate renewal option**, the individual certificate renewal email will be sent to the stakeholders with two links:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

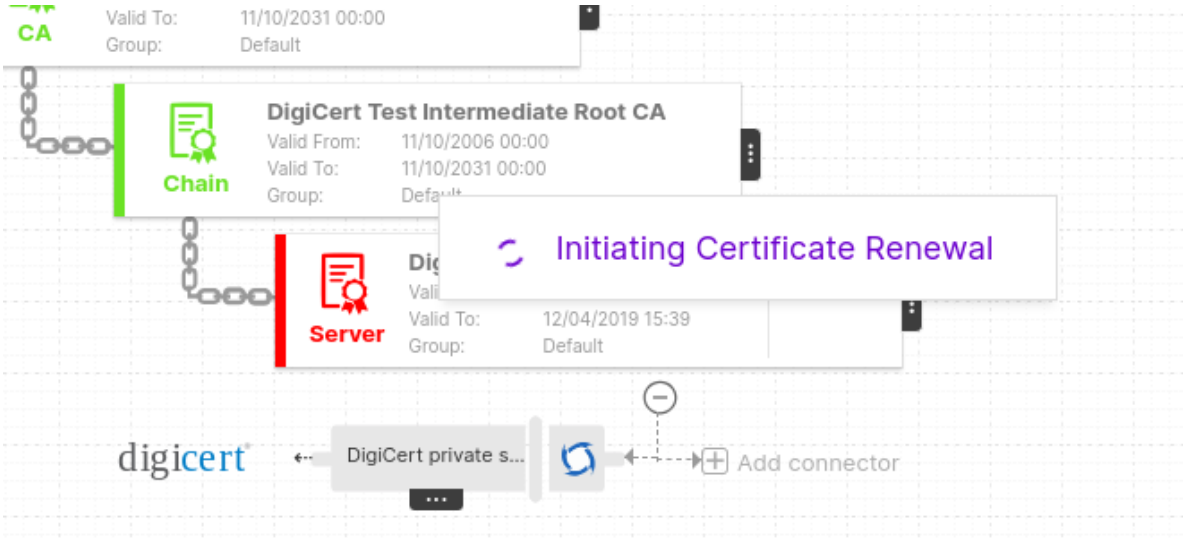
- Link for certificate renewal
- Link for unsubscribing from the alerts for that specific certificate

> **Tip:** You can repeat steps **4** to **9** to add more than one **Alert Configuration** under a **Alert Name**.

11. To renew the certificate:

    a. Click on the renewal link and login to AppViewX.

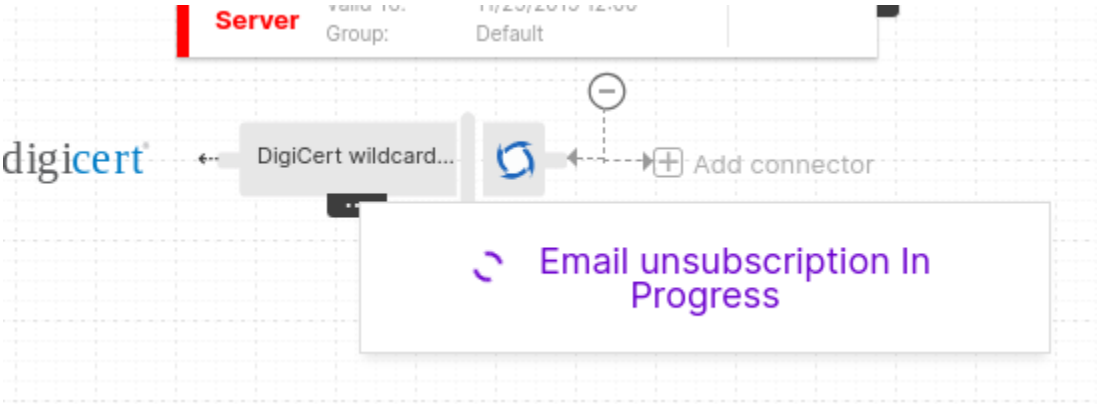
    You will be redirected to the holistic view for the certificate and the following renewal alert will be displayed:



    b. For instructions on how to renew a certificate, refer to the documentation for renewing a certificate.

    To unsubscribe from the alerts for the certificate, click the unsubscribe link from the alert email.

    You will be redirected to the certificate inventory page and the following unsubscribe alert will be displayed:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Certificate Expiry Alerts using Custom Workflows

You can create workflows with a customized configuration for the alert. Select the custom workflow at the time of creating the alert to bring it into effect.

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Expiry Alerts**.
   The **Expiry alert** inventory is displayed.
2. To create a new expiry alert using a custom workflow, click **+ Create**.
   The **Expiry Alert > Expiry Alert Add** page is displayed.

   Tip: This page has a list of best practices you are advised to follow when creating a new expiry alert.

3. For the new alert, enter a unique **Alert Name** (mandatory) and a description (optional) with additional details about the alert.
4. In the **Alert Configuration** section, click **+ Add**.
   The **Add Configuration** pane is displayed.
5. Select the **Certificate Type** for which you want to configure the expiry alert.
   - **End Certificate**
   - **CA Certificate**
6. Enter the **Filter Configuration** details.

Field descriptions for the Filter Configuration section

Field	Description
Certificate Expiry Period	To filter certificates based on their expiry: • **Range in days**: Sends an expiry alert email for certificates that will expire within the specified range of days from the current date For example, to set an alert for certificates that will expire between 10 and 40 days from the current calendar date, enter **10** and **40**. Alerts will be sent for all certificates expiring between 00:00:00 AM on the start day and 11:59:59 on the end day. • **On specified days**: Sends an expiry alert email for certificates that will expire on the nth day from the current date For example, to send an alert for certificates expiring on the 50th day from the current calendar date, enter **50**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Alerts will be sent for all certificates expiring between 00:00:00 AM and 11:59:59 PM of the specified day. • **Range in dates**: Sends an expiry alert email for all certificates expiring in a specific duration Use the calendar widget to select the **Start date** and **End date** for this duration. Alerts will be sent for all certificates expiring between 00:00:00 AM on the start date and 11:59:59 on the end date.
Additional Filters	To add a filter in addition to the certificate expiry period: a. Select the required filter from the **Select option** dropdown list. b. Enter the corresponding value in the **Type to enter value** field. c. Click **Add**. The selected filter option and its value are displayed.
***Notification Method**	To send an expiry alert using a custom workflow, select **Advanced**.
Ignore renewed/ regenerated certificate	When this field is enabled, results returned after the alert is triggered will not include certificates that have already been renewed or regenerated, even though they match the filter criteria.
***Custom workflow**	This field is displayed only when **Notification Method** = **Advanced**. From the dropdown list, select the required custom workflow.

7. Click **Add**.

   The created alert is listed in the table below the **+ Create** button.

> **Tip:** To edit/delete an alert, use the **Edit/Delete** button, as required.

8. Under **Alert Execution Type**:

> **Note:** The settings configured here will be applicable to all expiry alerts listed in the above table.

   a. To configure a manual alert that will be triggered immediately, select **Run Now** and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

OR

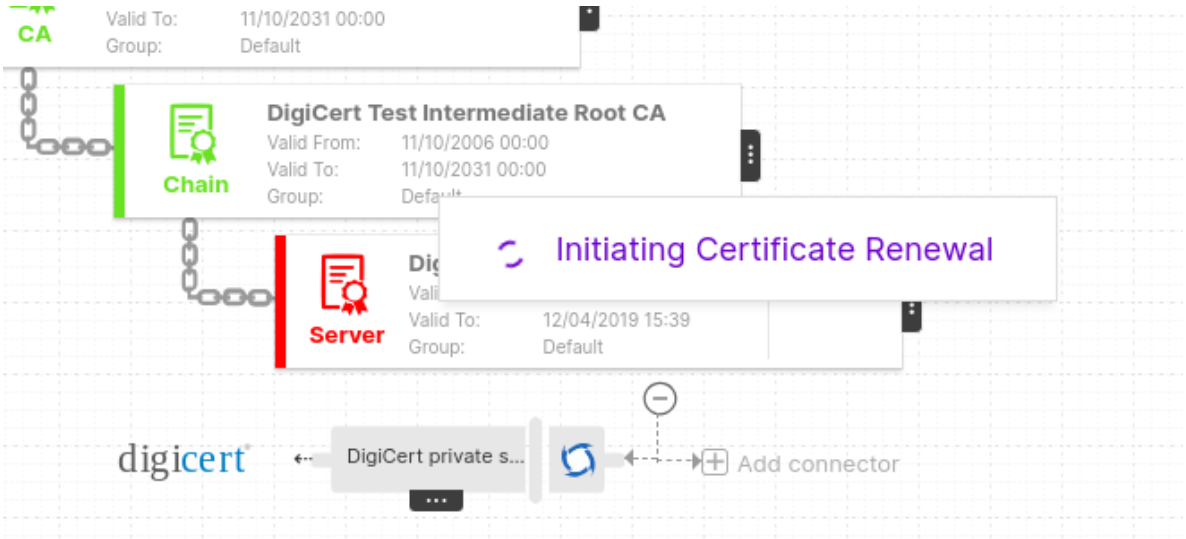
a. To trigger the alert at a scheduled time, select **Schedule** and enter the following details:
   - **Time Zone***
   - **Frequency** (daily/weekly/monthly/yearly)
   - **Starts On***
   - **Ends**
     - For ends **ON**, use the calendar widget to select the date on which the last expiry alert email will be sent.
     - For ends **After**, enter the number of **Occurrences** after which the expiry alert will be discontinued.

9. Click **Save**.
   Once the expiry alerts are configured with **Allow certificate renewal option**, the individual certificate renewal email will be sent to the stakeholders with two links:
   - Link for certificate renewal
   - Link for unsubscribing from the alerts for that specific certificate

> **Tip:** You can repeat steps **4** to **9** to add more than one **Alert Configuration** under a **Alert Name**.

10. To renew the certificate:

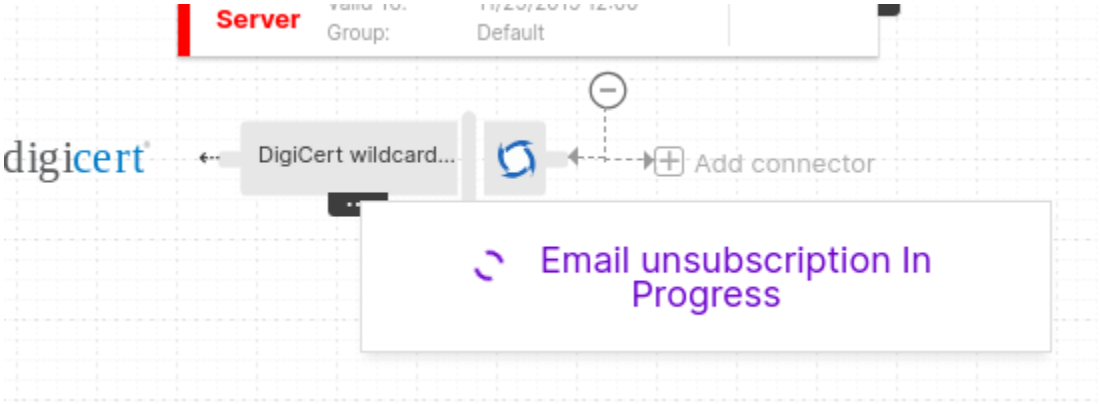
    a. Click on the renewal link and login to AppViewX.
    You will be redirected to the holistic view for the certificate and the following renewal alert will be displayed:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

b. For instructions on how to renew a certificate, refer to the documentation for renewing a certificate.
To unsubscribe from the alerts for the certificate, click the unsubscribe link from the alert email.

You will be redirected to the certificate inventory page and the following unsubscribe alert will be displayed:



Placeholders for Retrieving Certificate Details

To retrieve the certificate parameter values, you can use the following corresponding placeholders (on the right):

```
"common name" : "commonName",
    "country" : "country",
    "state" : "state",
    "location" : "location",
    "division" : "division",
    "organization" : "organization",
    "subject" : "subject",
    "mail address" : "mailAddress",
    "serial number" : "serialNumber",
    "valid from" : "validFrom",
    "valid until" : "validUntil",
    "directory names" : "enhancedSANTypes.directoryNames",
    "rfc822 names" : "enhancedSANTypes.rfc822Names",
    "registered IDs" : "enhancedSANTypes.registeredIDs",
    "uniform resource identifiers" : "enhancedSANTypes.uniformResourceIdentifiers",
    "dns names" : "enhancedSANTypes.dnsnames",
    "ip addresses" : "enhancedSANTypes.ipaddresses",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"ucc" : "enhancedSANTypes.ucc",
"fqdn" : "enhancedSANTypes.fqdn",
"other names" : "enhancedSANTypes.otherNames",
"upn" : "enhancedSANTypes.upn",
"issuer common name" : "issuer.commonName",
"issuer certificate authority" : "issuer.certificateAuthority",
"issuer setting name" : "issuer.settingName",
"issuer serial number" : "chainIdentifier.issuerSerialNumber",
"certificate group name" : "certificateGroup.name",
"vendor" : "certAssociations.vendor",
"device name" : "deviceDetails.deviceName",
"source" : "certAssociations.source",
"applications" : "certAssociations.applications",
```


Disabling Expiry Alerts Manually

1. Go to the certificate inventory and click the common name of the certificate that you want to disable the alerts for.
2. Set the **Expiry Alert** field to **False**.

Configuring a Certificate Expiry Alert

Certificate expiry alerts are sent to designated recipients for all certificates that are set to expire on the date specified on the Settings: Certificate expiry alert screen.

To configure a certificate expiry alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. Hover on **Alerts**, and then select **Configure Alerts**.
3. Enter a name for the certificate alert.
4. In the Event Type field, select Certificate Expiry Alert.
5. Select Critical as the severity of the alert.
6. Select the Certificate Category from the dropdown list.
7. In the Expires in (days) field, enter the number of days before a certificate expires. An alert will be sent out.
8. To use Email Configuration to send the alert, complete the following steps:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Select the Email Configuration checkbox.
- In the Email Address field, enter the email addresses you want to send the alert to. Use commas to separate the addresses.
- In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.

9. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
   - Enter the Destination IP for the alert.
   - Select the version of SNMP you want to use: V1 or V2.
   - Enter the port that should be used for the alert.
10. Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
11. Click Add to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Certificate Sync Alert

AppViewX maintains a record of what certificate is mapped to which Server:Application service, which can be seen on the certificate's holistic view. This information is used by AppViewX to monitor continued existence of the certificate on Server:Application. AppViewX establishes connectivity to the Server and validates if the Application is still configured with the Certificate. Any change in the status is flagged out as a Certificate Sync Alert. This can also be visualized through the change of Application Connector status color. The Application Connectors on the Certificate's holistic view will turn Red in such circumstances.

To configure a certificate sync alert:

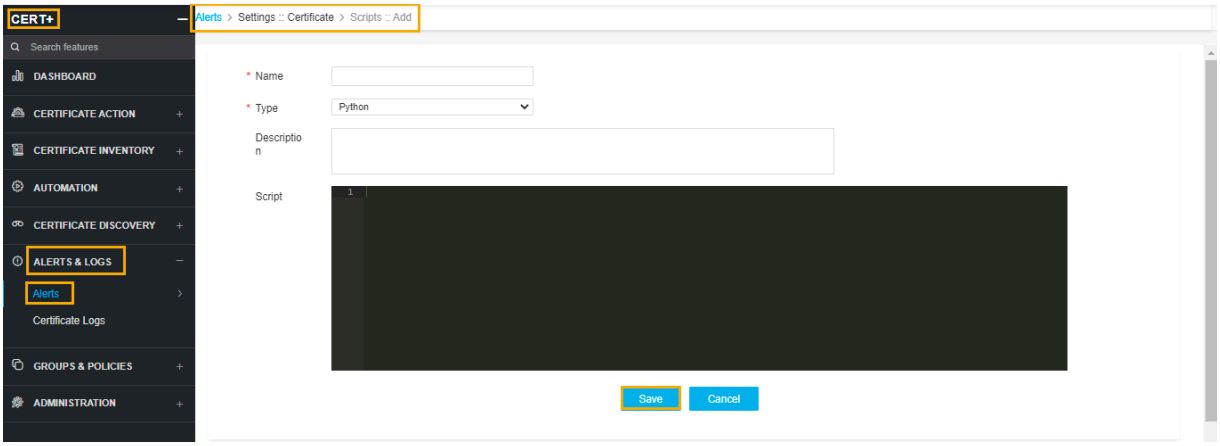
1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. In the **Event Type** field, select Certificate Sync Alert.
3. Enter/Select the alert details.

Field	Description
***Alert name**	Enter a unique name for the alert.
***Event type**	From the dropdown list, select **Certificate Sync Alert**.
***Vendor**	From the dropdown list, select the vendor for the alert criteria.

4. Enter a name for the certificate alert.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Select the Alert severity of the alert: Critical, Major, and Notification.
6. In the Alert Message field, enter the text that users see when the alert appears on the screen.
7. Select the Vendor whose device or application you are creating an alert for.
8. Select the Certificate Category from the dropdown list.
9. In the Device Name field, select the device associated with the certificate you are creating an alert for.
10. In the Application field, select the application associated with the certificate you are creating an alert for.
11. Select the Execute Script checkbox.
12. In the Execute Script dropdown list, select the script to trigger the alert. To create a script, click the (Add new script) icon. The below page appears.



- Provide value in the Name field.
- Type by default is selected as Python.
- Provide description value in the Description field.
- Enter the script to be executed in the Script field and click **Save**.

13. To use the Email Configuration to send the alert, complete the following steps:
    - Select the Email Configuration checkbox.
    - In the Email Address field, enter email addresses to send the alert to. Use commas to separate the addresses.
    - In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.
14. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Enter the Destination IP for the alert.
- Select the version of SNMP you want to use: V1 or V2.
- Enter the port that should be used for the alert.
- Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.

15. Click Add to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Certificate Validation Alert

AppViewX acts as a repository of all the known certificates in the organization. A certificate identifies a application via its Subject Common Name. In many a circumstance it observed that the organizations faces certificate related outages even if the certificate is valid. This is because of an error while setting up the application configuration or invalid certificate selected for the application. To identify such a misconfiguration AppViewX periodically validates the identity of application but trying and establishing connectivity to the Subject Common Name of server certificates in the Inventory. If the certificate is exchanged as part of SSL handshake is found to be invalid through expiry, revocation or through misconfiguration, AppViewX triggers a Certificate Validation Alert to notify administrators about a SSL handshake issue that users could be facing.

To configure a certificate validation alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. In the **Event Type** field, select **Certificate Validation** Alert.
3. Enter a name for the certificate alert.
4. Select the severity of the alert: Critical, Major, or Notification.
5. In the Alert Message field, enter the text that users see when the alert appears on the screen.
6. Select the Vendor whose device or application you are creating an alert for.
7. Select the Certificate Category from the dropdown list.
8. In the Device Name field, select the device associated with the certificate you are creating an alert for.
9. In the Application field, select the application associated with the certificate you are creating an alert for.
10. To use the Email Configuration to send the alert, complete the following steps:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Select the Email Configuration checkbox.
- In the Email Address field, enter email addresses to send the alert to. Use commas to separate the addresses.
- In the Subject field, leave the default text or enter the text that briefly describes the alert the user is receiving.

11. To use the Simple Network Management Protocol (SNMP) to send the alert, complete the following steps:
    - Enter the Destination IP for the alert.
    - Select the **version** of SNMP you want to use: V1 or V2.
    - Enter the port that should be used for the alert.
    - Enter the Community String for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
12. Click **Add** to create the alert. It then appears at the bottom of the screen and on the Certificate tab within the Alert module.

Configuring a Connection Failure Alert

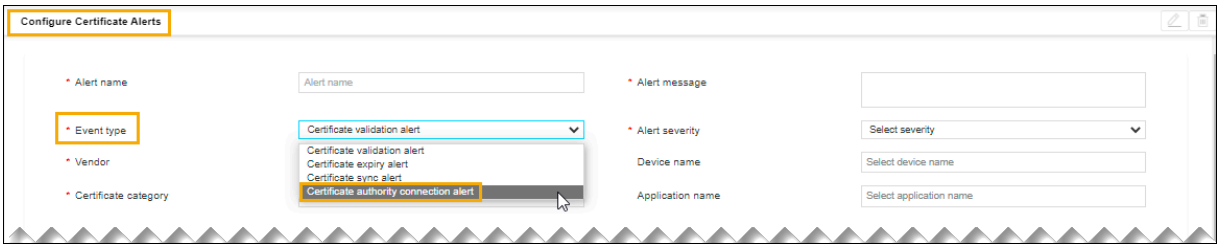
When a certificate is enrolled with AppViewX, a connection is established between the Certificate Authority (CA) signing the certificate. This connection is vital to perform CLM actions and certificate discovery tasks seamlessly.

When you can check manually if the connection is successfully established between AppViewX and certificate authority, and continues to stay so, starting version 2021.1.0, AppViewX allows you to configure automatic alerts when this connection fails. These alerts will be recorded in AppViewX logs as well as sent as email notifications.

To configure a connection failure alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Configure Alerts**.
   The **Configure Certificate Alerts** page is displayed.
2. Enter an **Alert name**.
3. From the **Event type** dropdown list, select **Certificate authority connection alert**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. From the **Certificate Authority Settings** dropdown list, select the CA Account
5. Set the **Alert severity** to critical.
6. To configure email alerts, in the **Email configuration** section, enter the **Email address** that will receive the email notifications in the event of a connection failure.
7. Enter the relevant subject in the **Subject** field.
8. To use the Simple Network Management Protocol (SNMP) for sending the alerts:
   a. Enter the **Destination IP** address for the alert.
   b. Select the SNMP **version** to be used.
   c. Enter the **Port** number to be used for the alert.
   d. Enter the **Community string** for the alert.

      The string is similar to a user ID or password and allows users to access the requested information on the device.
9. Click **Add** to create the alert.
   The new alert is now listed in the **Certificate Alerts** page.
10. Click **Reset** if you want to re-enter the details.

Configuring a CLM Action Failure Alert

A Certificate Lifecycle Management (CLM) action failure alert in certificate management is a notification generated when a CLM action fails. CLM involves managing digital certificates throughout their lifecycle, such as Enroll, Regenerate, Renewal, Revoke, Suspend, Reissue, and Reinstate.

When a CLM action fails, it means that a specific task related to certificate management did not complete successfully. These alerts inform administrators to investigate and resolve the problem, ensuring the

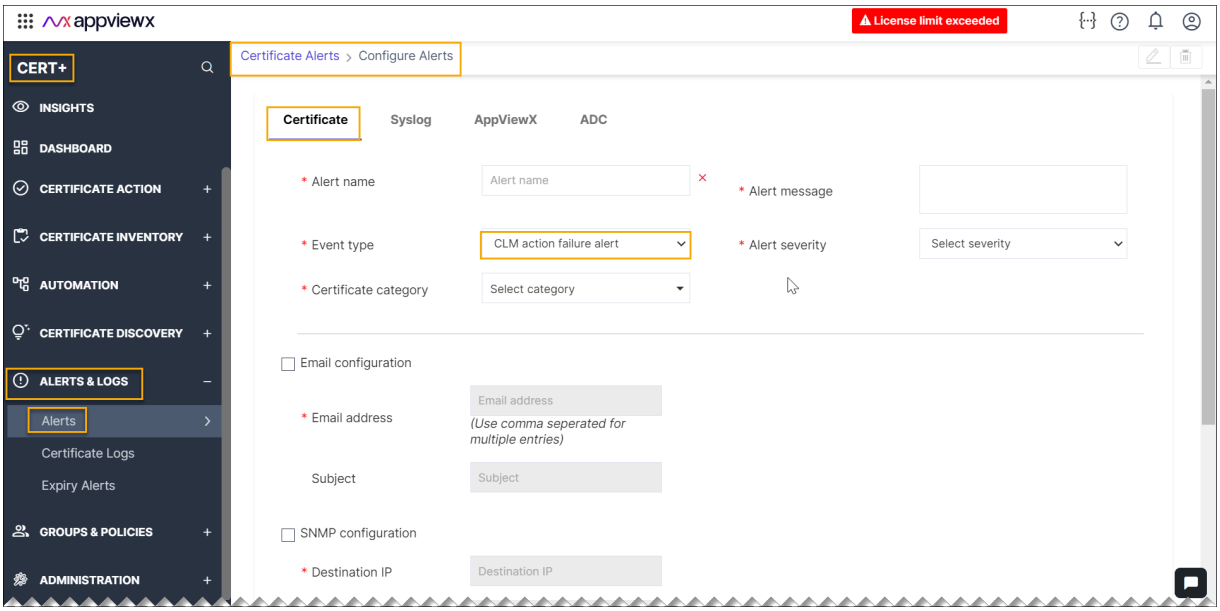
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

security and functionality of systems relying on digital certificates. This failure might happen due to various reasons, such as:

- **Network Issues**: Connectivity problems between the certificate authority (CA) and the requesting system.
- **Configuration Errors**: Incorrect settings or parameters within the certificate management system.
- **Authentication/Authorization Failures**: Issues with credentials or permissions required to perform the CLM action.
- **Expired Certificates**: Attempting to renew or use an expired certificate.
- **CA Service Problems**: Outages or issues with the CA providing the certificates.
- **Policy Violations**: Actions that do not comply with the defined security policies or certificate policies.

To configure a CLM action failure alert:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Alerts** > **Certificate Alerts**.
   The **Certificate Alerts** page is displayed.
2. Click the (⚙) **Settings** icon.
   The **Configure Alerts** page is displayed.
3. Enter an **Alert name**.
4. From the **Event type** dropdown list, select **CLM action failure alert**.



5. From the **Certificate category** dropdown list, select the type of certificate.
6. In the **Alert message** field, enter the additional information.
7. Set the **Alert severity** as required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. To configure email alerts, in the **Email configuration** section, enter the valid **Email address** that will receive the email notifications in the event of a connection failure.
9. Enter the relevant subject in the **Subject** field.
10. To use the Simple Network Management Protocol (SNMP) for sending the alerts:
    a. Enter the **Destination IP** address for the alert.
    b. Select the SNMP **Version** to be used.
    c. Enter the **Port** number to be used for the alert.
    d. Enter the **Community string** for the alert.

       The string is similar to a user ID or password and allows users to access the requested information on the device.
11. Click the **Add** button to create the alert.
    The new alert is now listed in the **Certificate Alerts** page, and below in the same **Configure Alerts** page.
12. Click **Reset**, if you want to re-enter the details.
13. Click **Cancel**, if you want to close **Configure Alerts** page and return to **Certificate Alerts** page.

Modifying the Configured CLM Action Failure Alerts

To ensure effective monitoring and timely resolution of issues in certificate management, you can modify the configured CLM (Certificate Lifecycle Management) action failure alerts.

To modify a CLM action failure alert:

1. In the **Configure Alerts** page > failure alerts list in bottom of page, click the check-box that the configured failure alert to be modified.
2. Once the check-box is selected, the **(** **) Modify** icon and **(** **) Delete** icon appears on the right-top of the page.
3. Click the **(** **) Modify** icon.
   The configure alerts page appears with existing information.
4. Enter the re-select/enter the required details in the fields.
5. Click **Update**.
   The pop-up appears as **Updated Successfully**.
6. Click **Cancel**, if you want to close **Configure Alerts** page and return to **Certificate Alerts** page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Deleting the Configured CLM Action Failure Alerts

You can delete the configured CLM action failure alerts from the certificate alerts list.

To delete a CLM action failure alert:

1. In the **Configure Alerts** page > failure alerts list in bottom of page, click the check-box that the configured failure alert to be modified.
2. Once the check-box is selected, the **(** **) Modify** icon and **(** **) Delete** icon appears on the rig- top of the page.
3. Click the **(** **) Delete** icon.
   The Confirmation window is displayed with message as **Do you want to delete certificate alert?**
4. Click **Yes**.
   The pop-up message appears as **Deleted Successfully**
5. Click **No**, if you want to return to **Configure Alerts** page.

Certificate Logs

Logs keep track of all activities that take place within AppViewX or any external entity that is connected to the AppViewX system. The Logging functionality in AppViewX tracks user activities and creates the device and object-level event logs. Certificate Logs helps you with logs that are related to certificates. Any system or certificate-related actions performed in the application are captured as logs. With these logs, you can check the system performance and it helps you with audit purposes to meet industry standards.

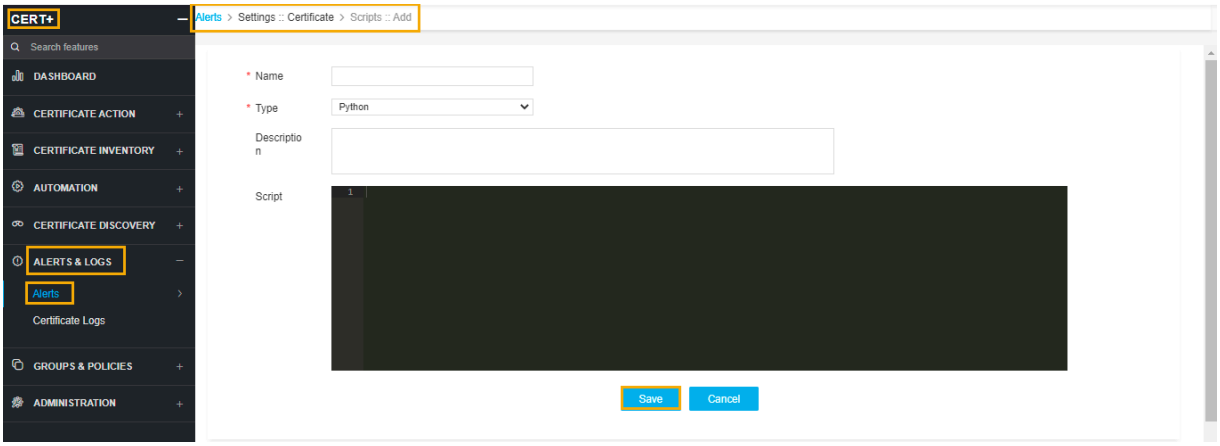
To check logs,

1. Log in to AppViewX application with valid credentials.
2. Click the menu button located in the upper left corner of the screen.

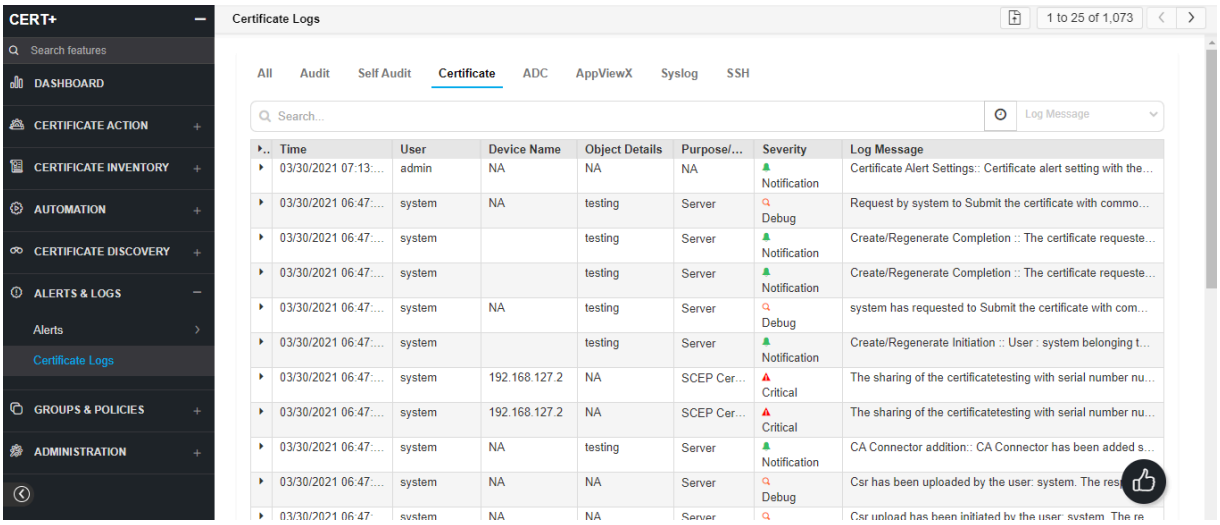
   The left navigation pane appears.
3. Click **CERT+**.

   The CERT+ left navigation pane appears.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. Under the section Alerts & Logs, select Certificate Logs.



5. On the Certificate logs list view page, you can find the list of logs related to the certificates. Any actions performed on the certificates are captured under this list view.
6. You can search for logs based on the time, user, device name, object details, and severity.
7. You can also filter logs based on the date and time and through the Log Message filter.
8. On the log screen, view all details for a log by hovering your cursor over each column of data or click the (Expand) icon for the log you want to view. The table row expands to display all details for the log.

Export Certificates Logs

When exporting logs in AppViewX, you can export all of the logs of a given type-for example, all Configure files or all Audit files-or you can search for specific logs or filter the default log list using the Date Range and Log Detail fields and then export only the logs that remain.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To export a logging report:

1. Go to (**Menu**) > **CERT+** > **ALERTS & LOGS** > **Certificate Logs**.
   The **Certificate Logs** page is displayed.
2. At the top of the Logging screen, click the tab for the type of logs you want to export: Certificate (in this case).
3. (Optional) Run a search for specific logs or filter the default list using the Date Range and/or Log Detail fields in the Search bar.
4. Click the export button in the Command bar in the top-right corner of the page.
5. The log report is then downloaded as a tar.gz file.

Managing Certificates Using Automation Workflows

AppViewX's predefined Out of the Box (OOB) workflows for CERT+ will assist you in self-servicing workflows for the certificate expiry notification, certificate enrollment, and certificate renewal. These workflows automate tasks like the intimation of expiry of certificates, generating reports of expiry of orphan certificates, updating certificate attributes, enrolling new certificates based on different input methods (manual, policy based, CSR), renewing and regenerating certificates, pushing certificates to devices, and incident automation with ServiceNow and JIRA.

The OOB tasks, available in the Workflow Studio, can be used to design workflows for certificate expiry notification, enrolling certificates, and renewing certificates as per your requirements.

- Getting Started
- Certificate Expiry Workflows
- Certificate Enrollment Workflows
- Renew Certificate Workflows
- Automation Workflow Tasks
- Designing a Custom Workflow using OOB Tasks
- Scheduling an OOB workflow
- Customizing an OOB Workflow

Getting Started

- Prerequisites
- Role-Based Access Control

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Accessing CERT+ Automation Workflows
• Accessing CERT Automation Work flow Tasks

Prerequisites

The following table describes the web browser requirements to create and execute workflows as well as tasks.

Web Browser Requirement

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	V74.0.1 (64-bit) or later
Google Chrome	V85.0.4183.83 (64-bit) or later

Role-Based Access Control

With role-based access control (RBAC), you can assign permissions to users for accessing the module and allow/restrict them to perform certain actions. You can refer to this link and find out more about RBAC.

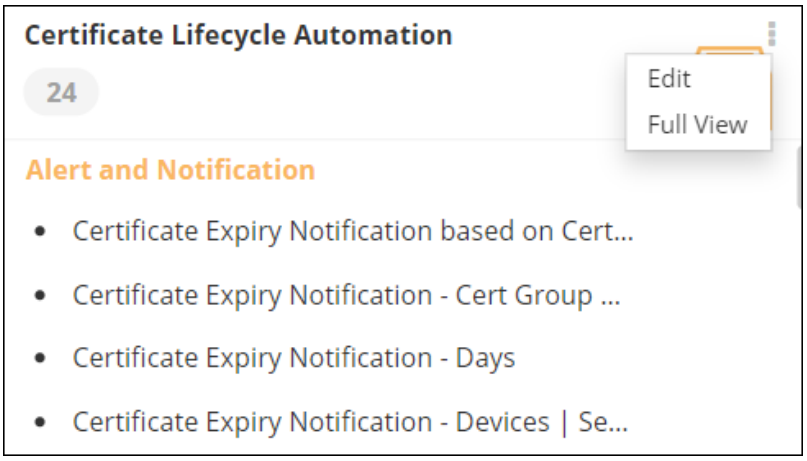
Accessing CERT+ Automation Workflows

You can access the CERT+ Automation workflows, available on the **Request :: View/Run** page, in the following ways:

- In the **CERT+** module, navigate to **AUTOMATION** > **My Workflows** > **View/Run**
- In the **Automation** module, navigate to **SERVICE REQUESTS** > **View/Run**

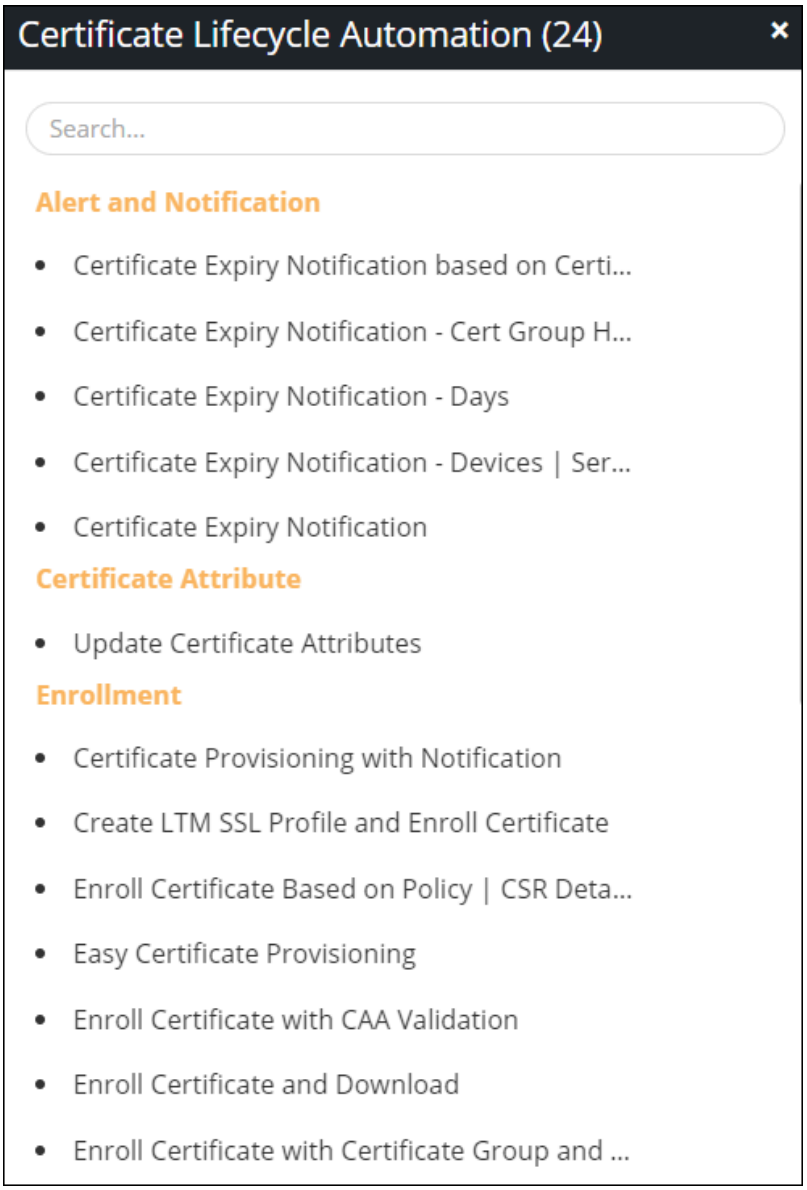
1. On the **Request :: View/Run** page, from the top right corner of the **Certificate Lifecycle Automation** catalog, click .
2. From the options displayed, select **Full View**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



The CERT+ Automation workflows are displayed in the **Certificate Lifecycle Automation** window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Tip: You can also search for a workflow on the **Catalog** page by typing the keyword(s) in the search bar.

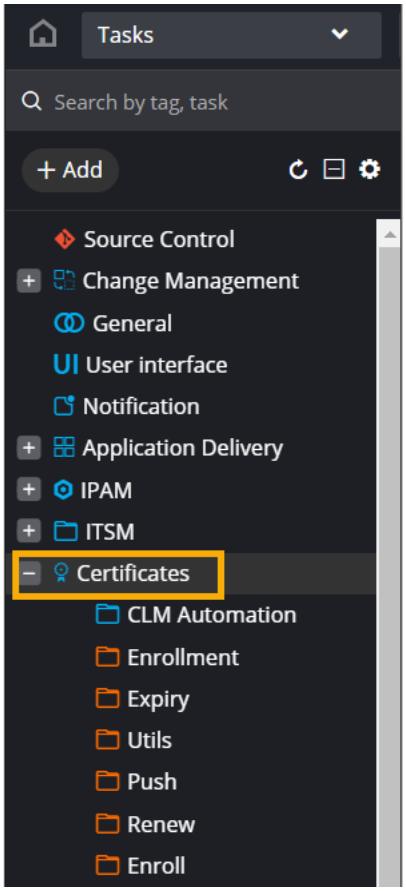
Accessing CERT Automation Work flow Tasks

The CERT+ Automation workflow tasks enable you to design your own custom workflows. These are available in the **Automation** module.

To view these tasks:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. In the **Automation** module, navigate to the **Workflow** page and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.
3. To access the OOB workflow tasks, from the left menu, expand **Certificates**.



The following categories of tasks are available in this folder:

- Enrollment - Lists all the OOB tasks for enrolling certificates from configured CAs.
- Expiry - Lists the Get Expiry Certificates task.
- Renew - Lists the Renew and Regenerate tasks.
- Push - Lists all the OOB tasks for pushing certificates to devices and servers.

Note: For more information on how to design a custom workflow using these OOB tasks, click here.

Certificate Expiry Workflows

- Overview
- Certificate Expiry Notification based on Certificate Attributes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

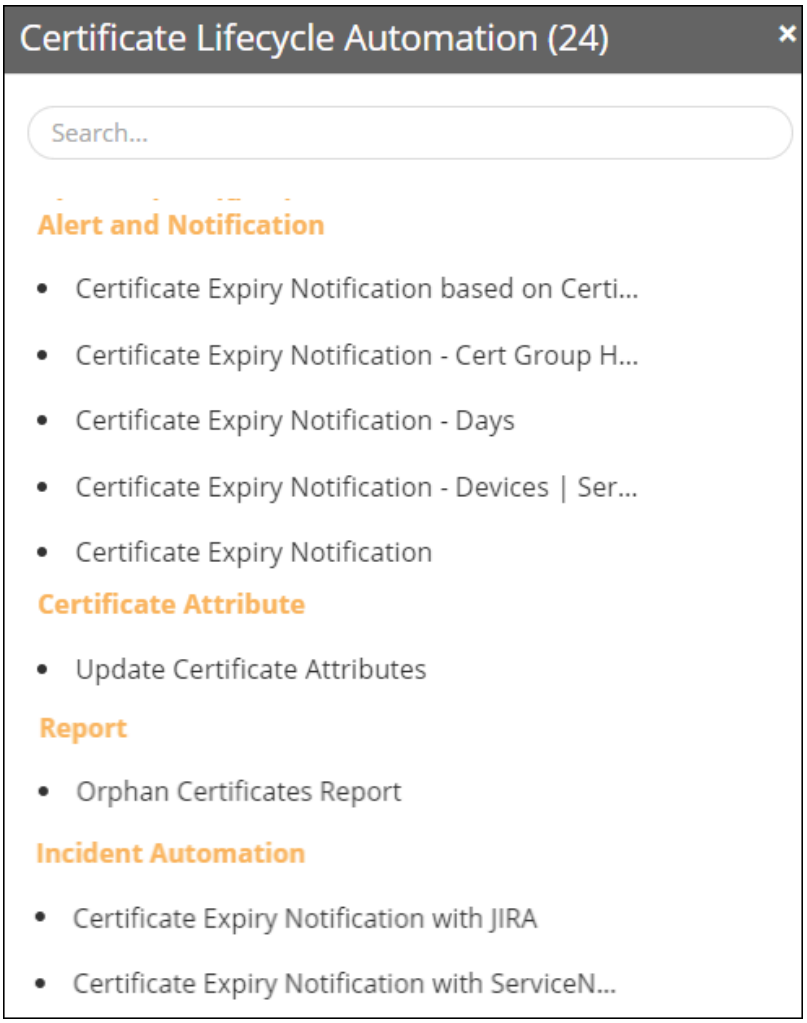
- Certificate Expiry Notification - Cert Group Hierarchy
- Certificate Expiry Notification - Days
- Certificate Expiry Notification - Devices | Servers
- Certificate Expiry Notification
- Update Certificate Attributes
- Certificate Expiry Notification with JIRA
- Certificate Expiry Notification with ServiceNow
- Orphan Certificates Report

Overview

This section lists and describes the workflows that can be used to notify the user(s) about the expiry of the certificates based on different criteria such as certificate attributes, expiry period, hierarchy, and so on. Some workflows also allow you to create tickets for expiring certificates on Jira/ServiceNow, update certificate attributes, and generate an orphan certificates report.

These workflows are available in the **Certificate Lifecycle Automation** catalog under four categories.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



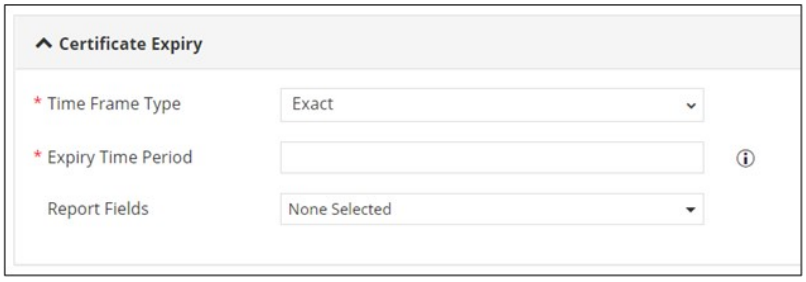
Certificate Expiry Notification based on Certificate Attributes

This workflow allows you to send an email notification listing certificates expiring in a specific number of days with selected certificate attribute details displayed in the email.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification based on Certificate Attributes** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

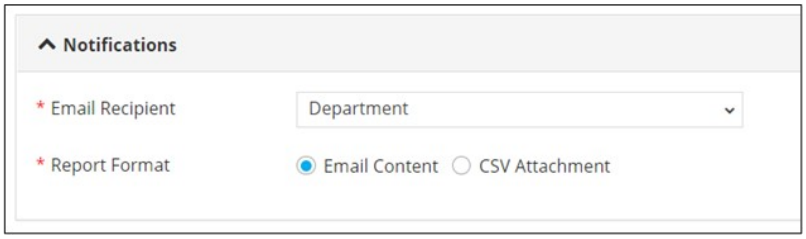


Field Description for Certificate Expiry section:

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact**: The system generates a report of certificates that expire on exactly the number of days as mentioned in the expiry time period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range**: The system generates a report of certificates that expire within a range of days as mentioned in expiry time period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.



Field Description in Notifications section:

Field	Description
***Email Recipient**	Select the email recipient from the dropdown list.
***Report Format**	Select the required checkbox to send the report as: • **Email content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The workflow is executed successfully and an email notification listing the certificates expiring in specific number of days with selected certificate attribute details is sent to the recipient email address(es) entered in the input form.

Certificate Expiry Notification - Cert Group Hierarchy

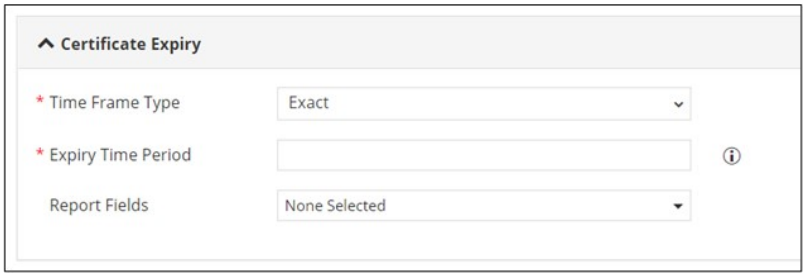
This workflow allows you to send a certificate expiry report notification to the certificate group and its associated hierarchical groups.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Cert Group Hierarchy** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

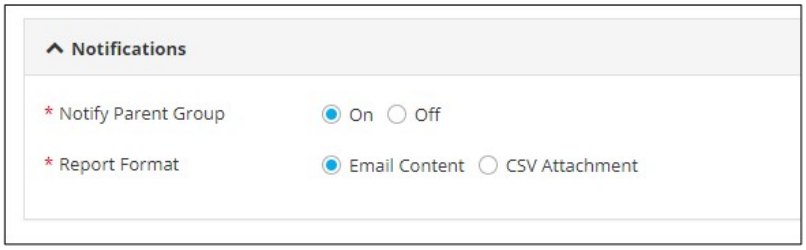


Field Description for Certificate Expiry section.

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact**: The system generates a report of certificates that expire on exactly the number of days as mentioned in the expiry time period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range**: The system generates a report of certificates that expire within a range of days as mentioned in expiry time period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field Description for Notifications section.

Field	Description
***Notify Parent Group**	Select: • **On** to send the notification to the certificate group's parent group. • **Off** if you don't want to send the notification to the certificate group's parent group. **Note: On** is the default selection.
***Report Format**	Select the required option to send the report as: • **Email content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   Workflow is executed successfully and a certificate expiry report notification is sent to certificate group and associated parent group(s).

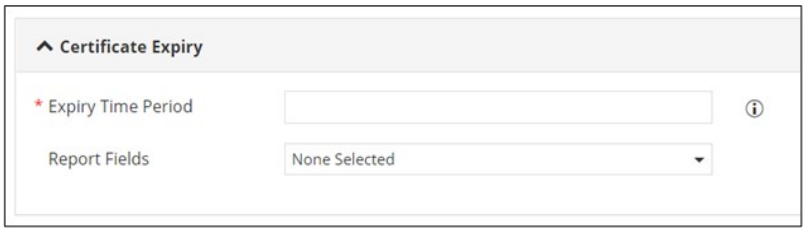
Certificate Expiry Notification - Days

This workflow enables you to generate a report listing certificates expiring in a specific number of days to the email addresses present in the certificate or certificate group.

To trigger this workflow:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

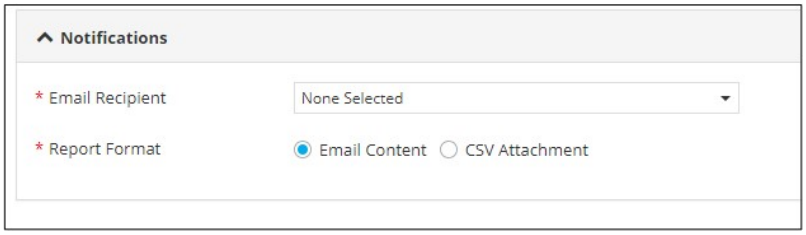
1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Days** workflow and click . The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.



Field Description for Certificate Expiry section.

Field	Description
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Notifications section.

Field	Description
***Email Recipient**	Select the required recipient of the notification. You can select: • **Select all** • **Certificate Email**: The notification will be sent to the email addresses associated with the certificate. • **Certificate Group Email**: The notification will be sent to the entire certificate group to which the certificate belongs.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The workflow is executed successfully and an email notification with a report listing certificates expiring in time period as specified in the input form is sent to the recipient email address(es).

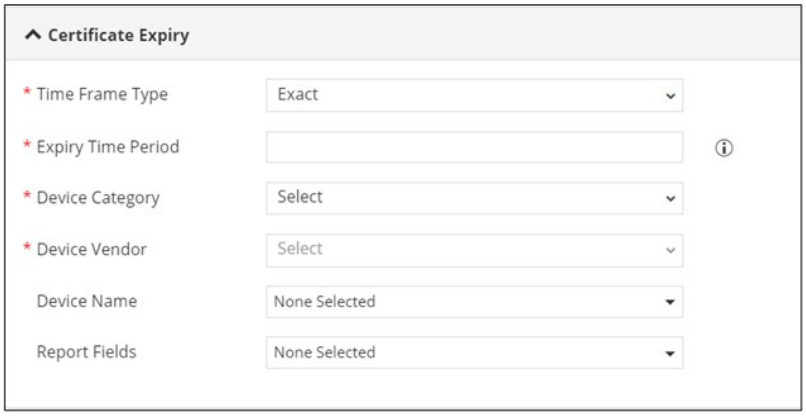
Certificate Expiry Notification - Devices | Servers

This workflow enables you to generate an expiry report of certificates present on a device and expiring in a specific number of days.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification - Devices | Servers** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



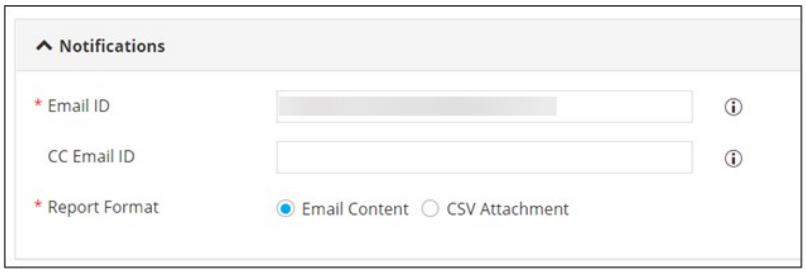
Field Description for Certificate Expiry section.

Field	Description
***Time Frame Type**	Enter the time frame type from the available options: • **Exact**: The system generates a report of certificates that expire on exactly the number of days as mentioned in the Expiry Time Period starting from today. For example, if you mention 30 in the Expiry Time period on the 1st day of the month, the report will contain details of certificates expiring on the 30th day of the month. • **Range**: The system generates a report of certificates that expire within a range of days as mentioned in Expiry Time Period. For example, if the range is mentioned as 30-60 on the 1st day of the month, the system generates a report of certificates expiring from 30th day to 60th day from that day. **Note: Exact** is the default selection.
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
***Device Category**	Select the device category for the report from the dropdown list.
***Device Vendor**	Select the device vendor for the report from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Device Name	Select the specific device for the report.
Report Fields	Select the report fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.



Field Description for Notifications section.

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.

   The workflow is executed successfully and an email notification with the list of devices and certificates present on that device expiring in a specific number of days is sent.

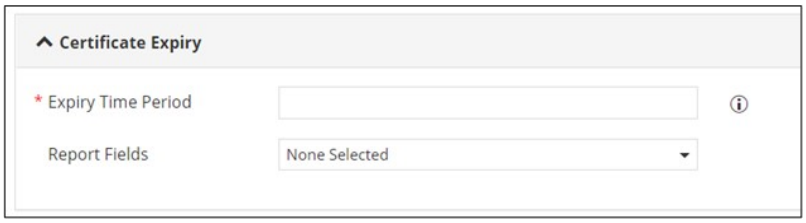
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Expiry Notification

This workflow enables you to generate a report listing certificates expiring in a specific number of days and notify the recipients via email. You can also mention email addresses of the recipients who need to be informed additionally in CC mails.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Expiry** section, enter or select the requested field information as described in the table below.

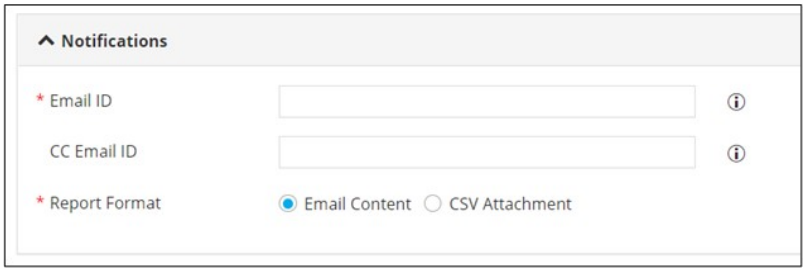


Field Description for Certificate Expiry section.

Field	Description
***Expiry Time Period**	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Report Fields	Select the fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field Description for Notifications section.

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma-separated values can be entered for multiple email addresses.
CC Email ID	Enter the email address of the additional recipients in the 'CC' field. Comma-separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**: The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The workflow is executed successfully and email notification listing certificates expiring in a specific number of days is sent to the email address(s) configured in the workflow input form.

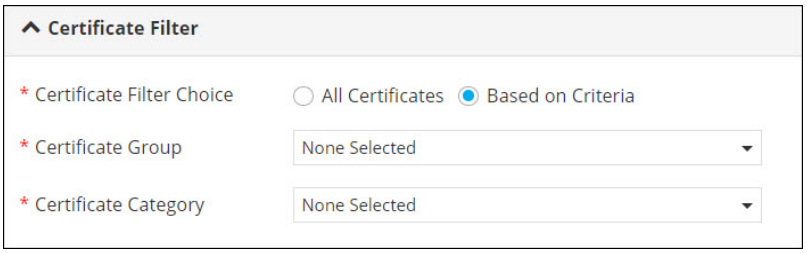
Update Certificate Attributes

This workflow allows you to update the certificate attributes in bulk.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Alert and Notification** category, hover your mouse over the **Update Certificate Attributes** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Certificate Filter** section, enter or select the requested field information as described in the table below.

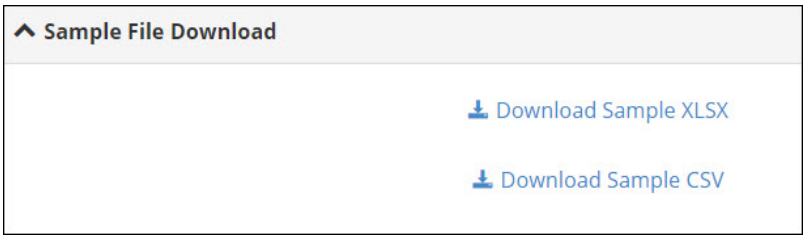
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field Description for Certificate Filter section.

Field	Description
***Certificate Filter Choice**	Select the required checkbox to fetch: • **All certificates**: This is the default selection and will fetch all the certificates. • **Based on Criteria**: Select this option to fetch certificates based on criteria such as certificate group and certificate category.
***Certificate Group**	Select the appropriate certificate group from the dropdown list. **Note:** This field is displayed only when you select the **Based on Criteria** option in **Certificate Filter Choice**.
***Certificate Category**	Select the appropriate certificate category from the dropdown list. **Note:** This field is displayed only when you select the **Based on Criteria** option in **Certificate Filter Choice**.
All asterisk (*) marked fields are mandatory.	

3. Click **Submit**.
   Certificates are fetched based on the selection criteria.
4. In the **Update Certificate Attribute Input** stage of workflow execution, select the option for downloading the file as a CSV or Excel file.



The file is downloaded to your device. You can now update the certificate attributes in this file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Once you have updated the certificate attributes, under **File Upload**, click to upload the modified file.

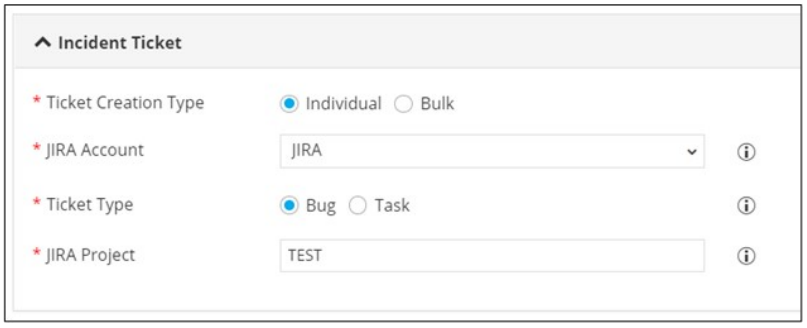
6. Click **Next** and in the **Confirmation** pop-up window, click **Ok**.
   The **Update Certificate Status** stage of the workflow displays the list of updated certificates. To download this list, from the top right corner of the screen, click . An email report is also sent to the requester.

Certificate Expiry Notification with JIRA

This workflow allows you to create a JIRA incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with JIRA** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Incident Ticket** section, select the requested field information as described in the table below.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Incident Ticket section.

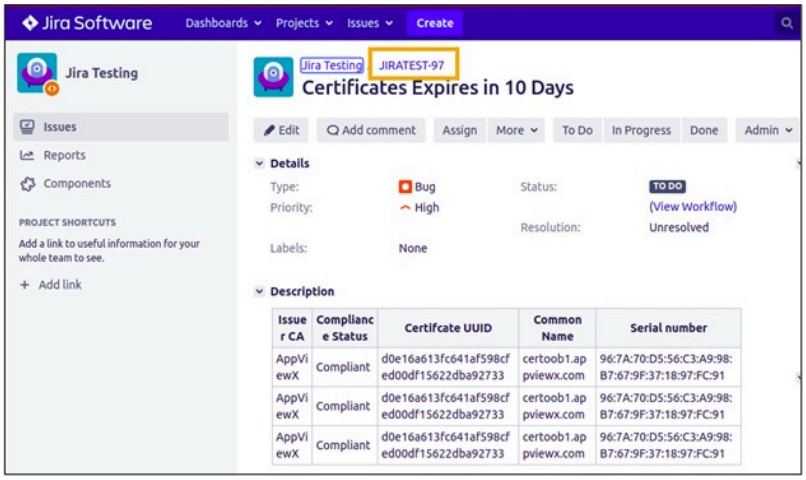
Field	Description
***Ticket Creation Type**	Select **Ticket Creation Type** as: • **Individual**: A separate ticket will be created for each certificate. • **Bulk**: A single ticket will be created for all the expiring certificates as per the category. The categories can be configured based on the ticket priority as Low, Medium and High. **Note: Individual** is the default selection.
***JIRA Account**	Select the **JIRA Account** as configured in the Integration Hub from the options available in the dropdown. **Note: JIRA** is the default selection.
***Ticket Type**	Select the type of ticket with reference to the project: • **Bug**: This will indicate that the ticket is for a bug in the project. • **Task**: This will indicate that the ticket is for a task in the project. **Note: Bug** is the default selection.
***JIRA Project**	Enter the name of the project for which ticket(s) have to be raised. **Note: Test** is the default selection.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
4. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for tickets with medium priority. For example, for certificates expiring in 60 days, incident priority can be medium.
5. Under the **High - Set Incident ticket Priority** section, enter a value (number of days) for tickets with high priority. For example, for certificates expiring in 30 days, incident priority can be high.
6. Under the **Description Fields** section, select certificate attributes from the dropdown that will be displayed in the JIRA issue description.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: This is a mandatory field. Multiple certificate attributes can be displayed by selecting the checkbox of the attribute name.

7. Click **Submit**.
   The **Ticket Creation Summary** stage of workflow execution displays the JIRA ticket ID and the ticket for Certificate expiry notification is created on JIRA.

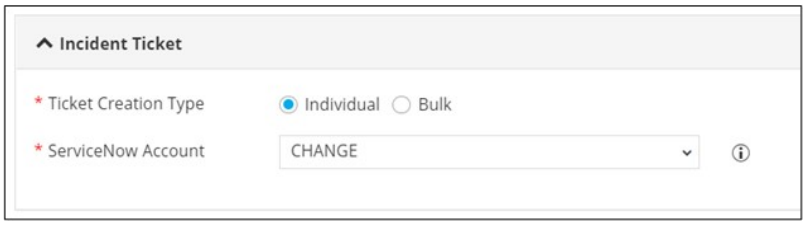


Certificate Expiry Notification with ServiceNow

This workflow allows you to create a ServiceNow incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with ServiceNow** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Incident Ticket** section, select the field requested information as described in the table below.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Incident Ticket section.

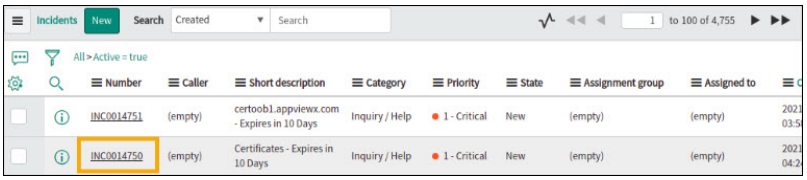
Field	Description
***Ticket Creation Type**	Select **Ticket Creation Type** as: • **Individual**: A separate ticket will be created for each certificate. • **Bulk**: A single ticket will be created for all the expiring certificates as per the category. The categories can be configured based on the ticket priority as Low, Medium and High. **Note: Individual** is the default selection.
***ServiceNow Account**	Select the **ServiceNow Account** as configured in the Integration Hub from the options available in the dropdown. **Note: Change** is the default selection.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
4. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for tickets with medium priority. For example, for certificates expiring in 60 days, incident priority can be medium.
5. Under the **High - Set Incident ticket Priority** section, enter a value (number of days) for tickets with high priority. For example, for certificates expiring in 30 days, incident priority can be high.
6. Under the **Description Details** section, select multiple certificate attributes from the dropdown that will be displayed in the ServiceNow description.

   Note: This is a mandatory field.

7. Click **Submit**.

   The **Ticket Creation Summary** stage of workflow execution displays the ServiceNow ticket ID and the ticket for Certificate expiry notification is created on ServiceNow.



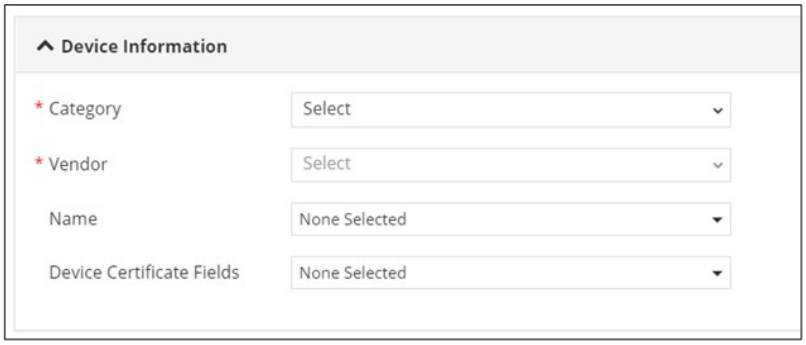
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Orphan Certificates Report

This workflow enables you to generate a report on certificates that are present on a device but not associated with any application or profile.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Report** category, hover your mouse over the **Orphan Certificates Report** workflow and click .
   The workflow is executed with the workflow inputs requested at the first stage.
2. Under the **Device Information** section, enter or select the requested field information as described in the table below.



Field Description for Device Information section.

Field	Description
***Category**	Select the device category for the report from the options available in the dropdown.
***Vendor**	Select the device vendor for the report from the options available in the dropdown.
Name	Select the specific device for the report.
Device Certificate Fields	Select the report fields to be displayed in the report from the dropdown list.
All Asterisk (*) marked fields are mandatory.	

3. Under the **Notifications** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Notifications section.

Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
***Report Format**	Select the required checkbox to send the report as: • **Email Content**:The report will be sent as Email content. • **CSV Attachment**: The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

4. Click **Submit**.
   The **Orphan Certificates List** is generated and an email notification is sent to the recipients specified in the input form.

Certificate Enrollment Workflows

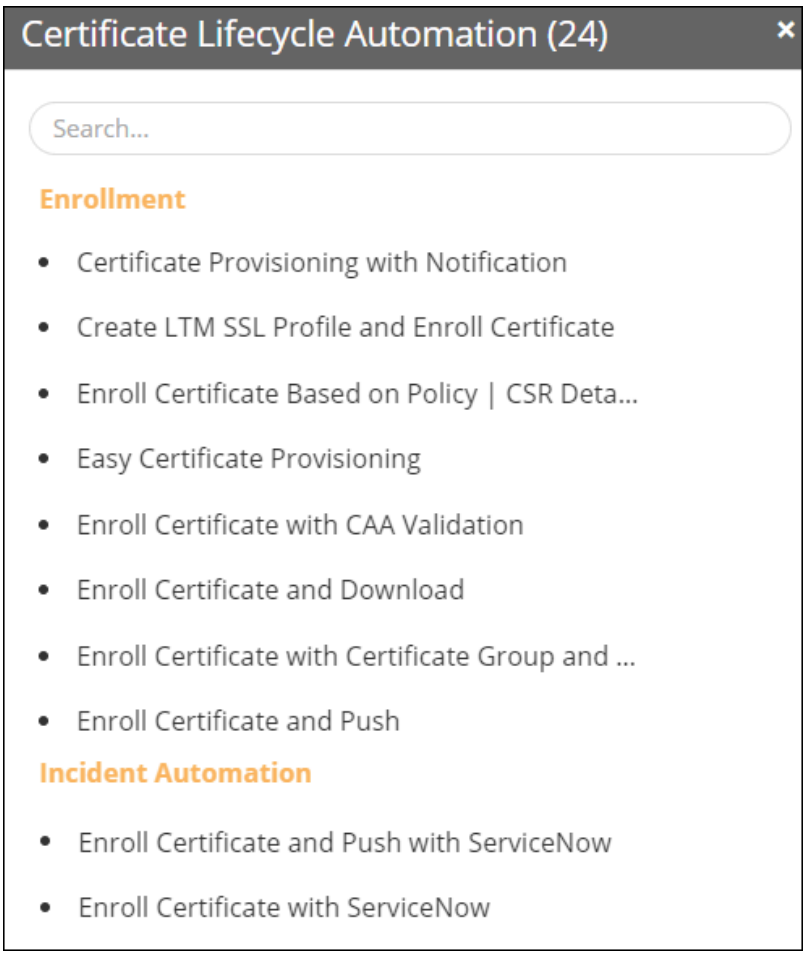
- Overview
- Enroll Certificate and Download
- Certificate Provisioning with Notification
- Enroll Certificate Based on Policy | CSR Details | CSR Upload
- Create LTM SSL Profile and Enroll Certificate
- Enroll Certificate with Certificate Group and CSR Upload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Enroll Certificate With ServiceNow
- Enroll Certificate and Push with ServiceNow
- Easy Certificate Provisioning
- Enroll Certificate with CAA Validation
- Enroll Certificate and Push

Overview

This section lists and describes the workflows that can be used to enroll certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Enrollment with Incident Automation. These workflows are available in the **Certificate Lifecycle Automation** catalog under the **Enrollment** and **Incident Automation** categories.



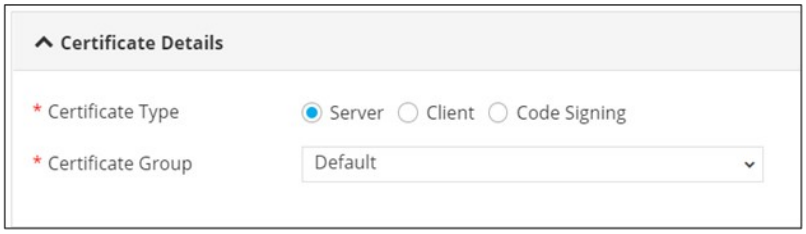
Enroll Certificate and Download

This workflow enables you to create and download certificates based on the certificate group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

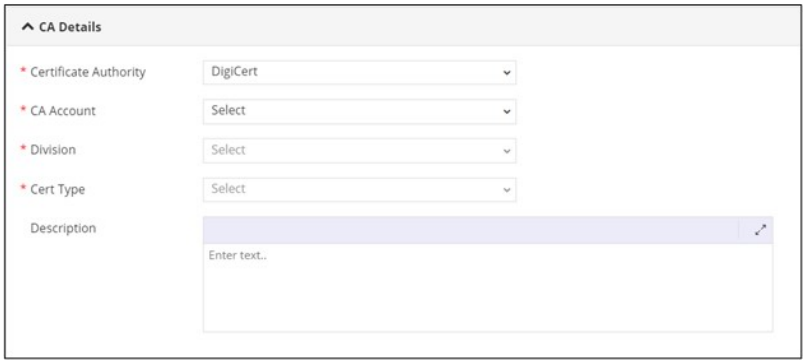
1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Download** workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.



Field description for Certificate Details section

Field	Description
***Certificate Type**	Select the required **Certificate Type** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information as described in the table below.



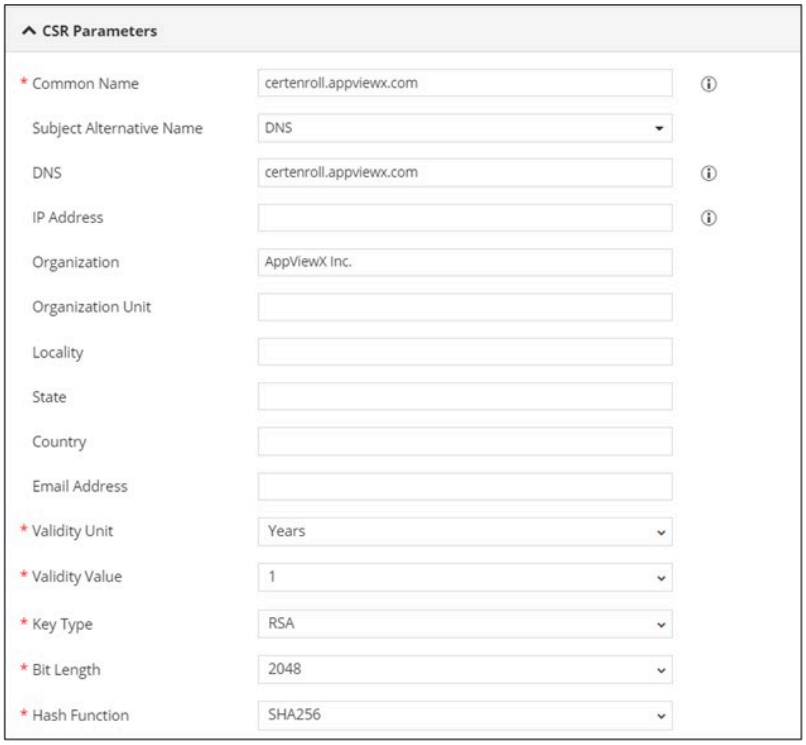
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note**: This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Enter a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



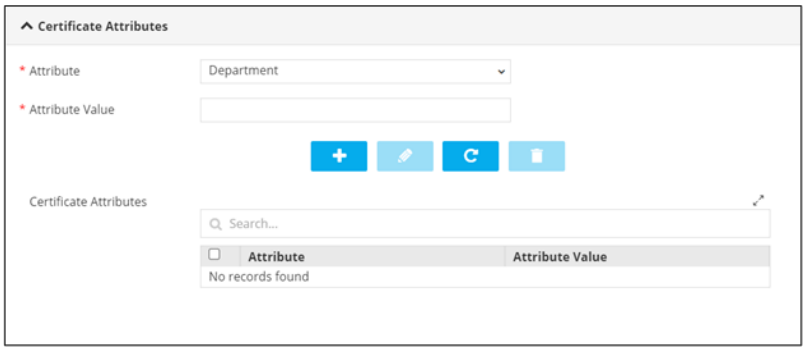
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS, if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP address, if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed in this section will vary based on the CA selected.

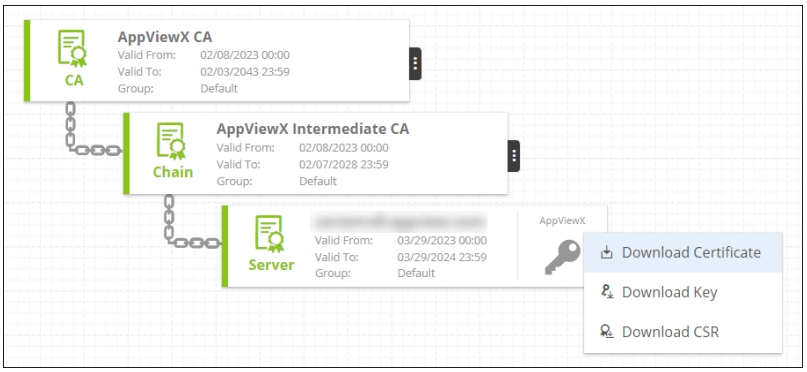
8. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** This field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

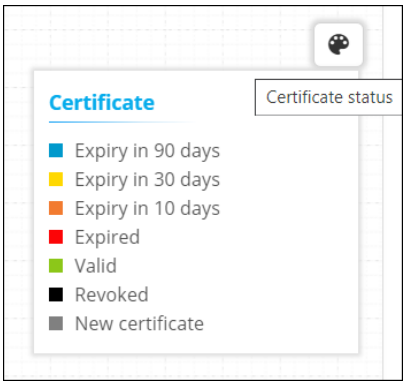
9. Click **Submit**.
   The certificate is created successfully and an email notification is sent to the recipient specified in the input form.

10. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



11. Hover your mouse over to view the Certificate status.



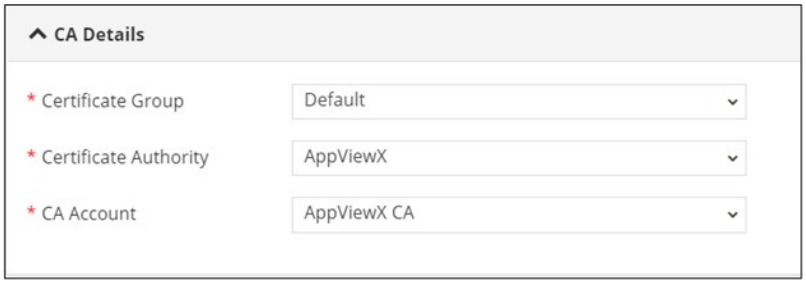
Certificate Provisioning with Notification

This workflow allows you to create a certificate based on the certificate group and the policy associated with it, and push to a device available in the instance. Email approval is required for certificate creation as well as pushing it to the device. Once approved, the logged in user will receive an email informing them about the Push to Device Status of the certificate.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Certificate Provisioning with Notification** workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field description for CA Details section

Field	Description
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the selected **Certificate Group**.
CA Account	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **CA**selected .
All asterisk (*) marked fields are mandatory.	

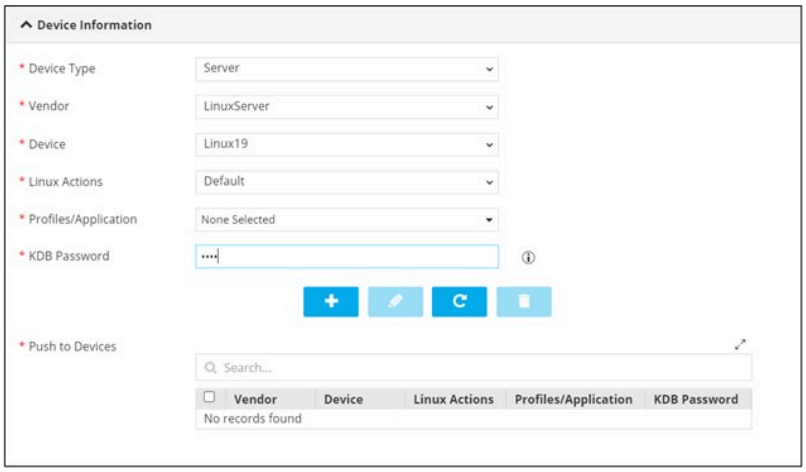
3. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Type	Select the Subject Alternative Type from the available options: • DNS • IP Address
Subject Alternative Name	Enter a valid Subject Alternative Name.
All Asterisk (*) marked fields are mandatory.	

4. Under the **Device Information** section, enter or select the requested field information as described in the table below.



Field description for Device Information section

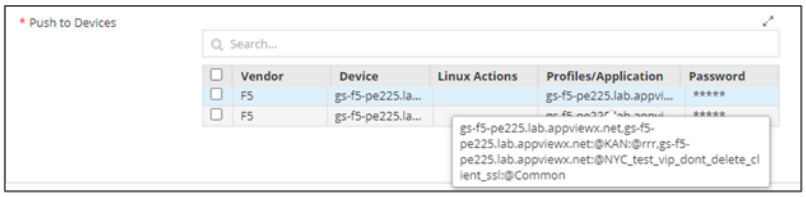
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the grid, click .
   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

6. Under the **Email** section, enter the field information as described in the table below.

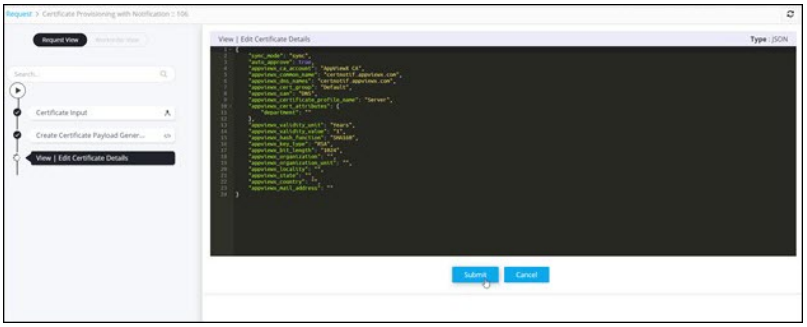
Field description for Email section

Field	Description
***Certificate Approver Email ID**	Enter the email address or multiple addresses, separated by comma, of the user(s) approving the certificate creation request.
***Certificate Push Approver Email ID**	Enter the email address of the user who will approve the certificate push request.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.

   The workflow is executed successfully.

8. At the **View | Edit Certificate Details** stage, click **Submit**.



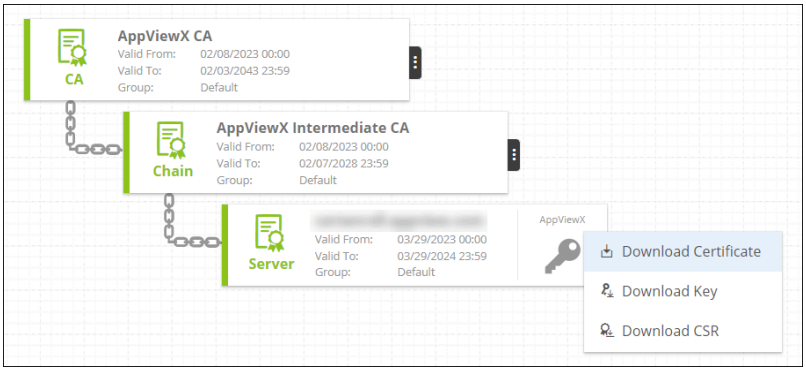
   Email notification for Create Certificate approval is received.

9. Click **Approve** or **Reject** in the **Approval for Creating Certificate** email.

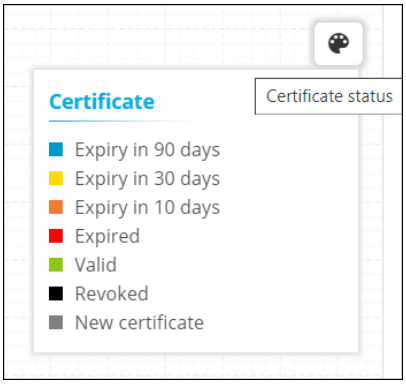
   Certificate is created after the approver clicks **Approve**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over , and from the options displayed, click **Download Certificate**.



11. Hover your mouse over to view the Certificate status.



12. Click **Approve** or **Reject** in the **Approval for Pushing Certificate to Device** email.

Once the approver approves the request, the certificate is pushed to the selected device and an email notification is also sent to the requester.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

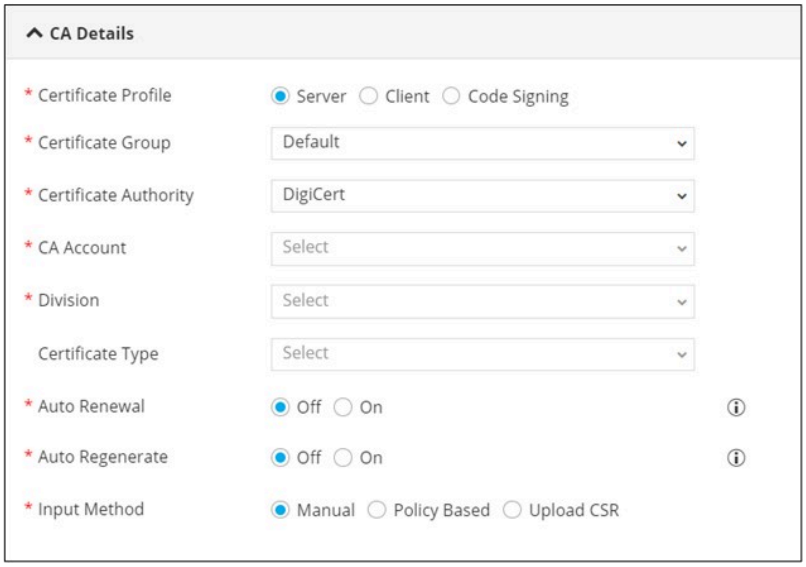
Enroll Certificate Based on Policy | CSR Details | CSR Upload

This workflow allows you to create a certificate using three input methods - Manual, Policy Based, and Upload CSR.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate Based on Policy | CSR Details | CSR Upload** workflow and click .

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.



Field description for CA Details section

Field	Description
***Certificate Profile**	Select the Certificate Profile from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert is selected as the CA.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
***Auto Regenerate**	Select the required radio button to enable/disable **Auto Regenerate**. **Note:** Default selection is set to **Off**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Start Regenerating (Days)	Enter the number of days in the **Start Regenerating (days)** field. **Note:** This field is displayed only when the **Auto Regenerate** field is enabled.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual**: (Default) If you select the **Input Method** as **Manual**, the CSR parameters will have to be entered/selected manually. For instructions, click here. • **Policy Based**: If you select the **Input Method** as **Policy Based**, the CSR parameter fields will be auto-populated based on the policy associated with the selected **Certificate Group**. For instructions, click here. • **Upload CSR**: If you select the **Input Method** as **Upload CSR**, you can upload the CSR file to fetch the CSR parameters. For instructions, click here.
All Asterisk (*) marked fields are mandatory.	

Enrolling Certificates Based on Input Method

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Field description for CSR Parameters section

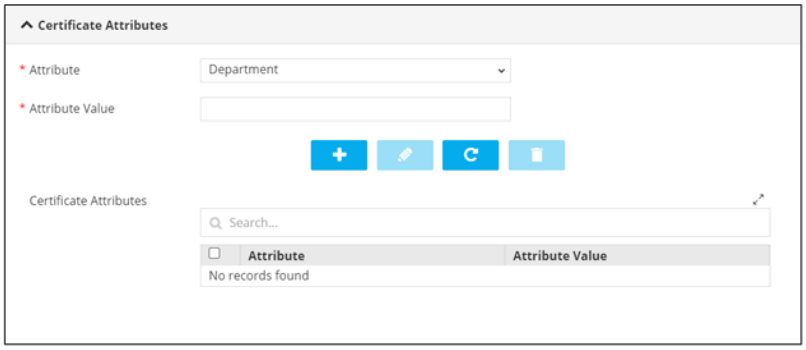
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

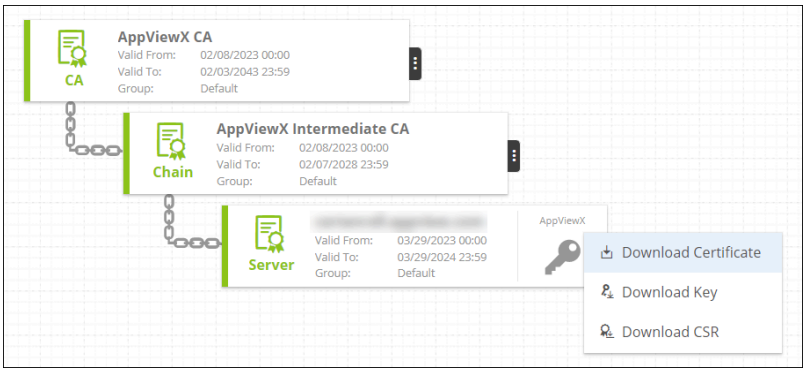
Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.
5. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

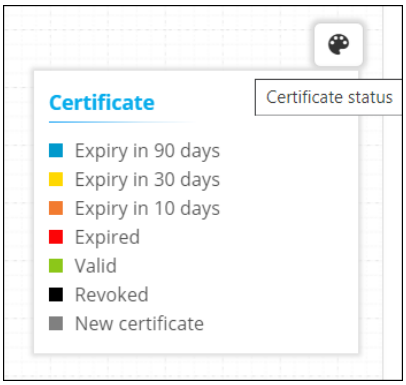
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

6. Click **Submit**.
   AppViewX certificate is created successfully and an email notification is sent to the recipient specified in the input form.
7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



8. Hover your mouse over to view the **Certificate status**.



Policy Based

After you select the **Input Method** as **Policy Based**, execute the following steps to enroll a certificate:

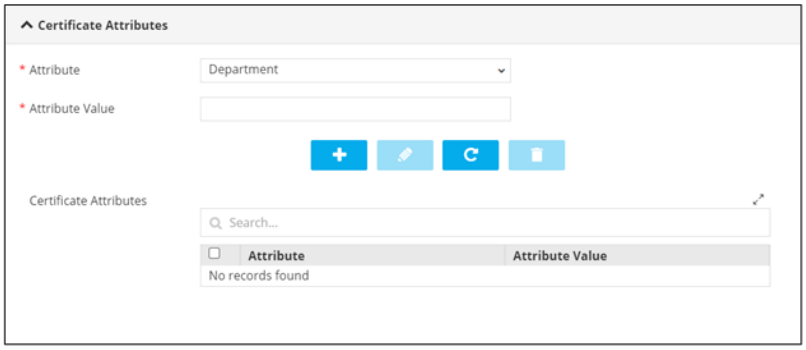
1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

> **Note:** Some CSR Parameters will be auto-populated based on the policy associated with the **Certificate Group**.

> **Note:** For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

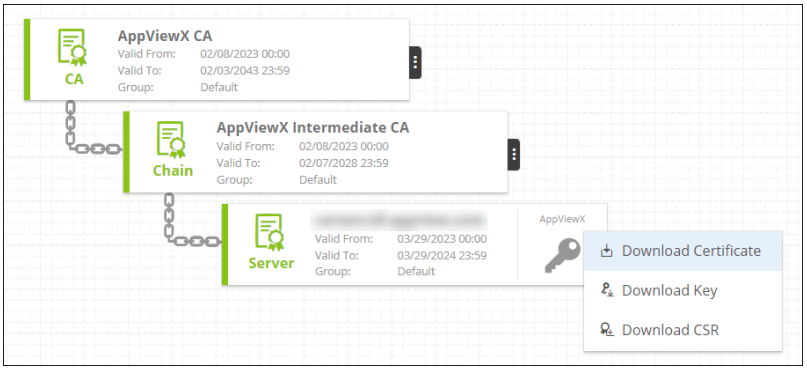
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

6. Click **Submit**.

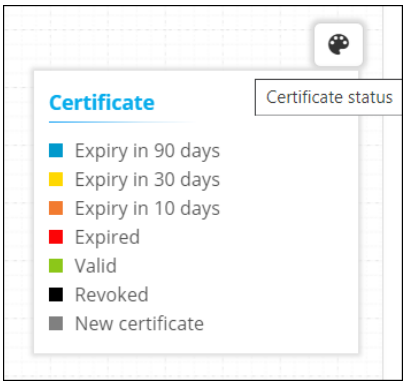
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX certificate is created successfully and email notification is sent to the recipient specified in the input form.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



8. Hover your mouse over to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

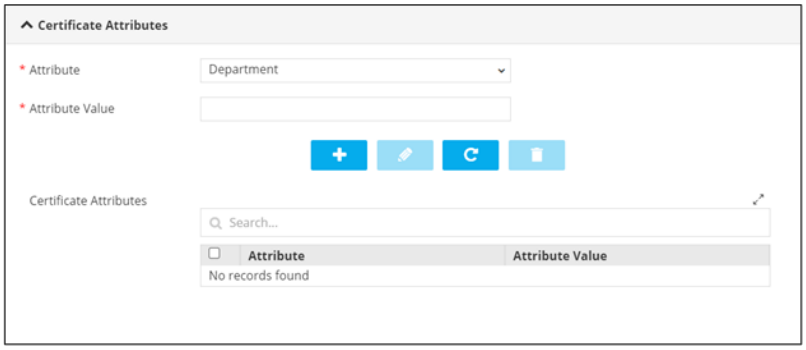
1. Under the **CSR Parameters** section, to **Upload CSR**, click .

2. Click **Fetch CSR Parameters**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.
✎	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click ✎, enter the new value for the attribute, and click ✎ again.
🗑	Allows you to delete a certificate attribute.
⤢	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

Note: This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

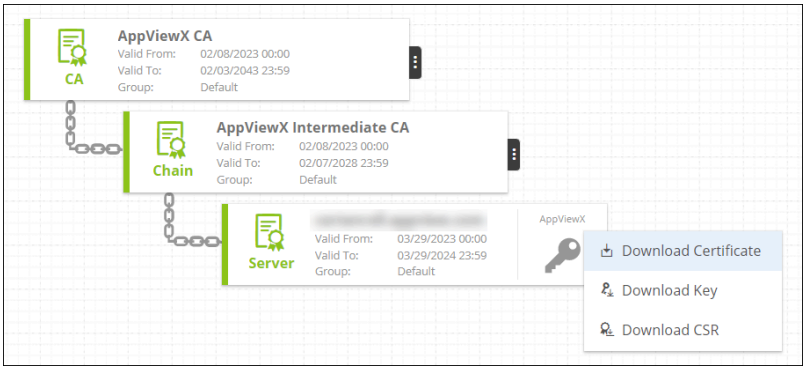
6. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

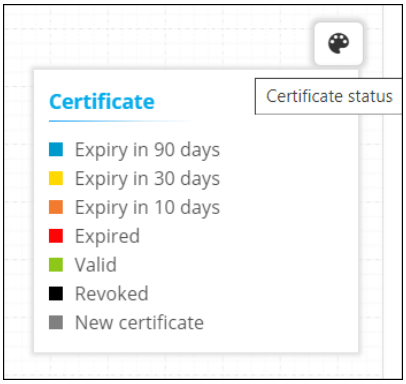
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.
   AppViewX certificate is created successfully and email notification is sent to the recipient specified in the input form.

8. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



9. Hover your mouse over to view the **Certificate status**.



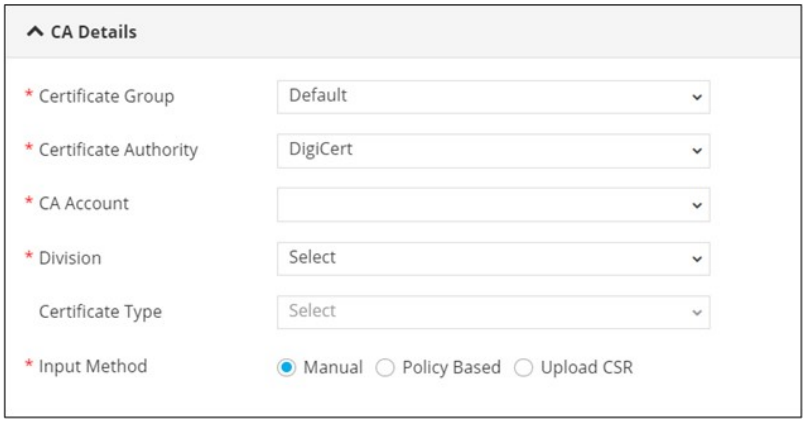
Create LTM SSL Profile and Enroll Certificate

This workflow allows you to create individual server certificates along with LTM SSL profile creation based on the selected certificate group.

To trigger this workflow:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Create LTM SSL Profile and Enroll Certificate**workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.



Field descriptions in the CA Details section

Field	Description
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** The **Certificate Authority** field is populated based on the selected **Certificate Group**.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** The **CA Account** field is populated based on the selected **Certificate Authority**.
***Division**	Select the **Division** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual**: (Default) If you select the **Input Method** as Manual, the CSR parameters will have to be entered/selected manually. For instructions, click here. • **Policy Based**: If you select the **Input Method** as Policy Based, the CSR parameters fields will be auto-populated based on the policy associated with the selected **Certificate Group**. For instructions, click here. • **Upload CSR**: If you select the **Input Method** as Upload CSR, you can upload the CSR file to fetch the CSR parameters. For instructions, click here.
All asterisk (*) marked fields are mandatory.	

Enrolling Certificates Based on Input Method

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

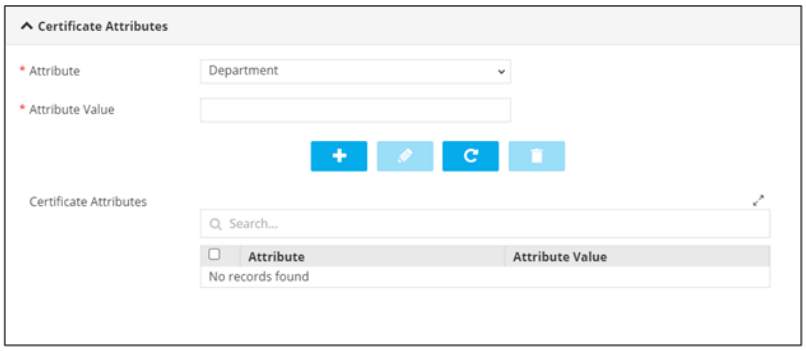
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field. **Note:** This field is displayed if DNS is selected in the **The email id of the logged in user is populated automatically.** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field. **Note:** This field is displayed if IP Address is selected in the **Subject Alternative Name** field.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

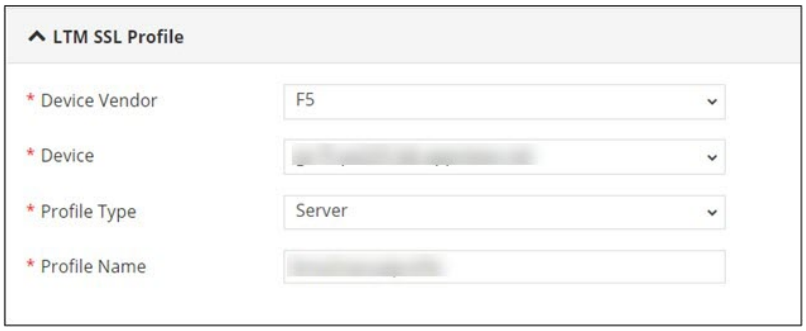
Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **LTM SSL Profile** section, enter or select the requested field information as described in the table below.



Field description for LTM SSL Profile section

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

6. Under the **Notifications** section, enter the email address(es).

> **Note:** The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

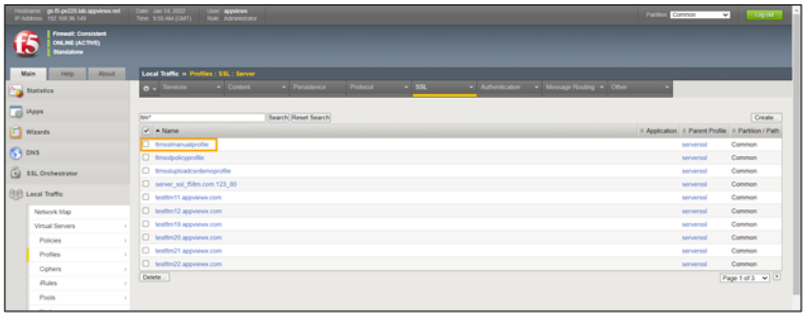
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Click **Submit**.

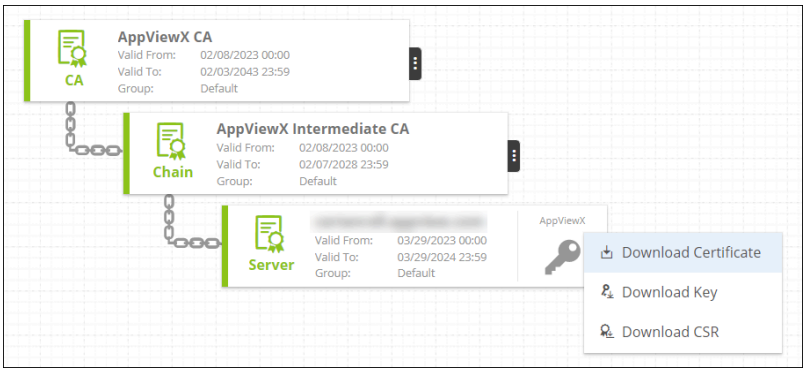
   AppViewX Certificate is generated and LTM Profile on Server SSL is created successfully.
8. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

   Note: You can change the profile name at this stage.

   LTM Profile is created and pushed to the selected F5 device and an email notification is sent to the recipient specified in the input form.

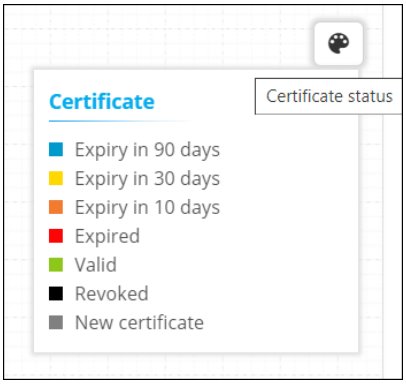


9. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. Hover your mouse over to view the **Certificate status**.



Policy Based

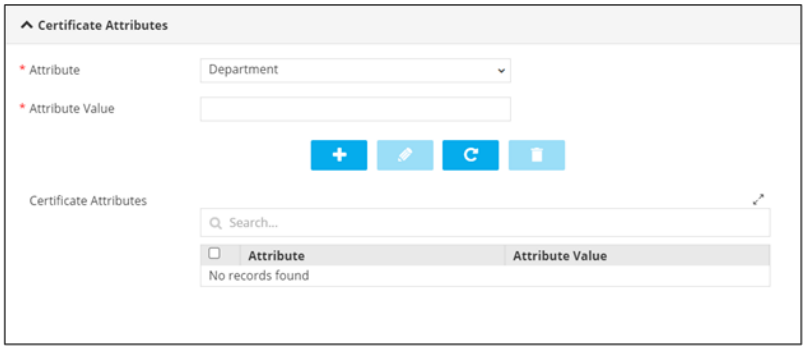
After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

> **Note:** Some CSR Parameters will be auto-populated based on the policy associated with the **Certificate Group**.

> **Note:** For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

5. Under the **LTM SSL Profile** section, enter or select the requested field information as described in the table below.

Field description for LTM SSL Profile section

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Under the **Notifications** section, enter the email address(es).

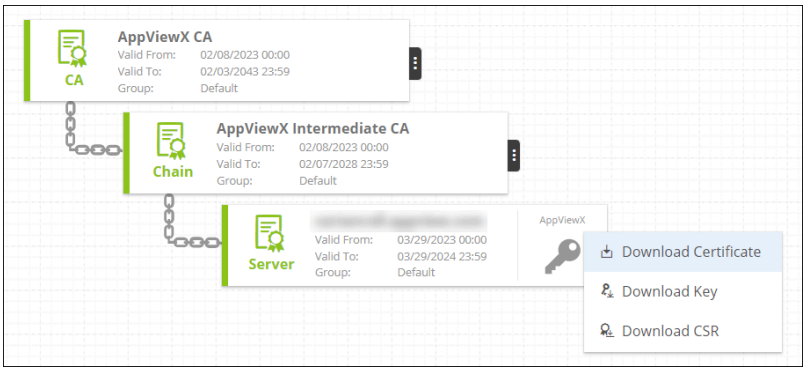
> **Note:** The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.
   AppViewX Certificate is generated and LTM Profile on Server SSL is created successfully.
8. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

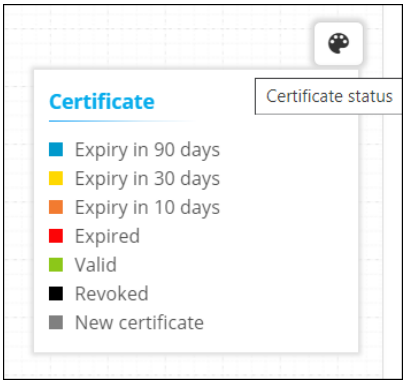
> **Note:** You can change the profile name at this stage.

   LTM Profile is created and pushed to the selected F5 device and an email notification is sent to the recipient specified in the input form.

9. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



10. Hover your mouse over to view the **Certificate status**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click .

2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.

Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.
✎	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click ✎, enter the new value for the attribute, and click ✎ again.
🗑	Allows you to delete a certificate attribute.
⤢	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

6. Under the **LTM SSL Profile** section, enter or select the requested field information as described in the table below.

Field description for LTM SSL Profile section

Field	Description
***Device Vendor**	Select the device vendor from the options available in the dropdown.
***Device**	Select the device from the options available in the dropdown. **Note:** This field is populated on the basis of the selected device vendor.
***Profile Type**	Select the profile type from the options available in the dropdown.
***Profile Name**	Enter a meaningful profile name for the profile that is to be created.
All asterisk (*) marked fields are mandatory.	

7. Under the **Notifications** section, enter the email address(es).

Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

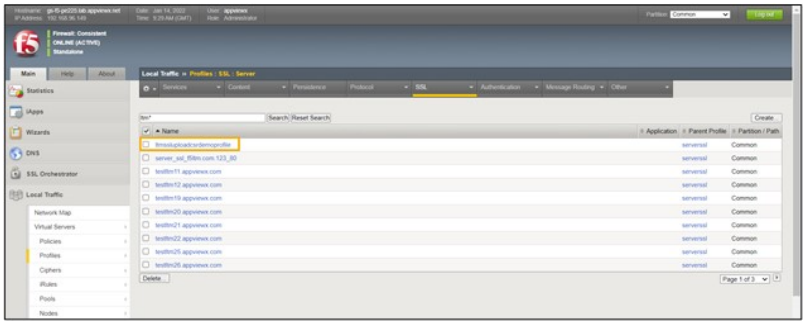
8. Click **Submit**.
   AppViewX Certificate is generated and LTM Profile on Server SSL is created successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

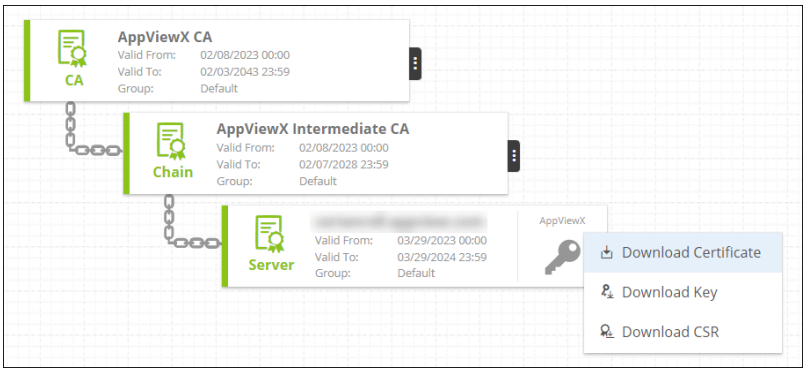
9. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

> **Note:** You can change the profile name at this stage.

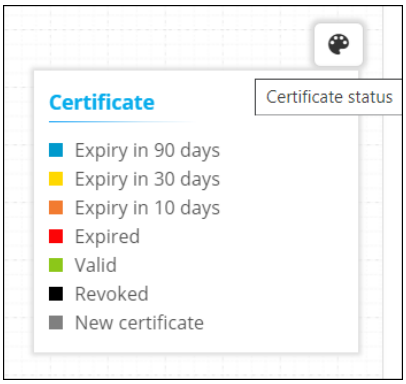
LTM Profile is created and pushed to the selected F5 device and an email notification is sent to the recipient specified in the input form.



10. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



11. Hover your mouse over to view the **Certificate status**.



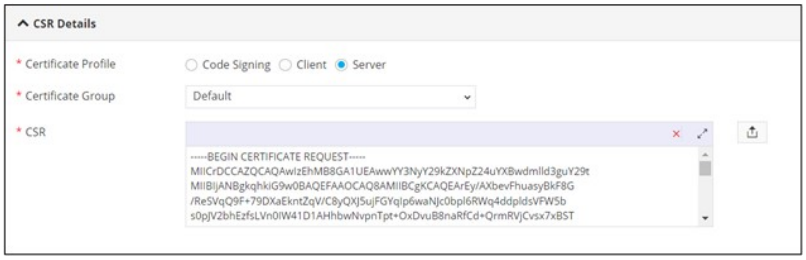
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enroll Certificate with Certificate Group and CSR Upload

This workflow allows you to create a certificate with minimal input. The Certificate Authority (CA) must be associated with the respective policy and Certificate group. In case there are multiple CAs associated with a policy, the first available CA will be considered for certificate creation.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with Certificate Group and CSR Upload** workflow and click . The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CSR Details** section, select the requested field information as described in the table below.



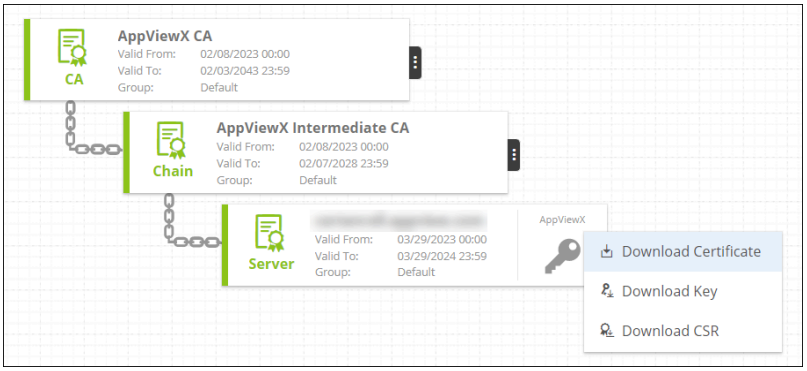
Field description for CSR Details section

Field	Description
***Certificate Profile**	Select the **Certificate Profile** from the following options: • **Code Signing** • **Server** • **Client** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***CSR**	Click to upload the **CSR** file.
All asterisk(*) marked fields are mandatory.	

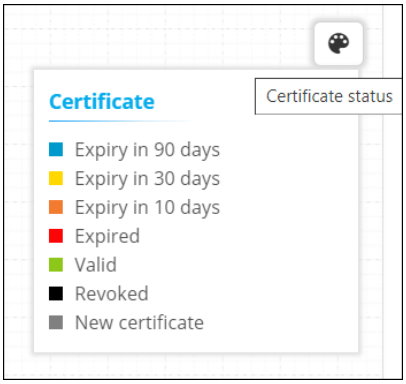
3. Click **Submit**.
   AppViewX Certificate is generated successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



5. Hover your mouse over to view the **Certificate status**.



Enroll Certificate With ServiceNow

This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM).

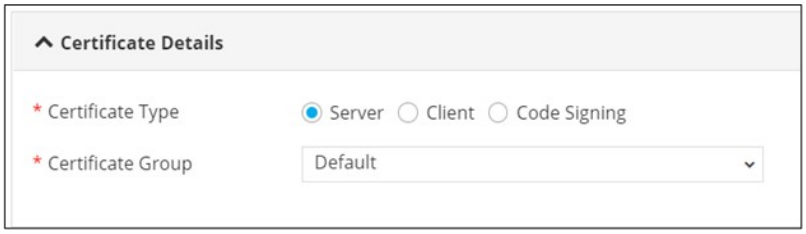
To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with ServiceNow** workflow and click .

> **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field description for Certificate Details section

Field	Description
***Certificate Profile**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*****) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information described in the table below.

Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when DigiCert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Provide a Description for the workflow, if required.
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter or select the requested field information described in the table below.

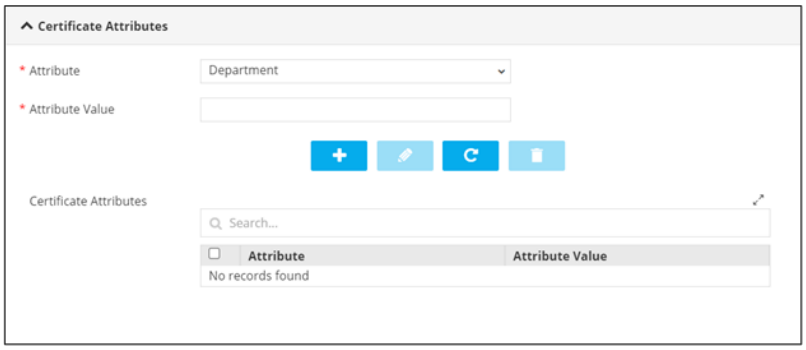
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully qualified domain name (FQDN) of the server for which the certificate is requested.
***Subject Alternative Name (SAN)**	Select the SAN as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
***Organization**	Enter the name of the organization .
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Organization Address	Enter the address of the organization.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Email Address	Enter the email address
Locality	Enter the name of the locality in which the organization is situated.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options - RSA, DSA, EC.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the Hash Function from the available options.
***Download Format**	Select the format for downloading the certificate from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

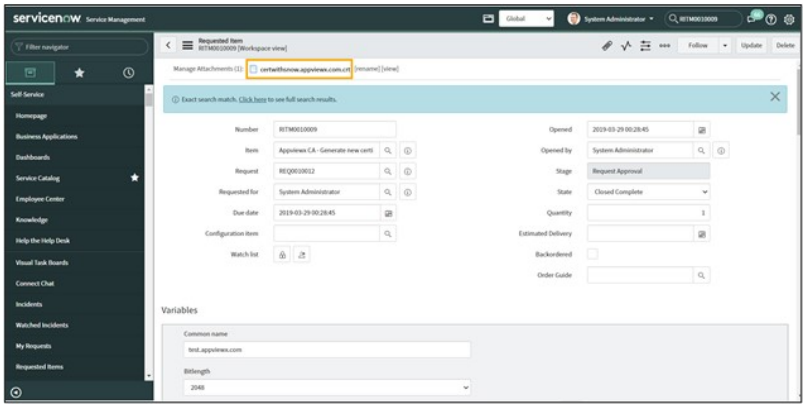
7. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

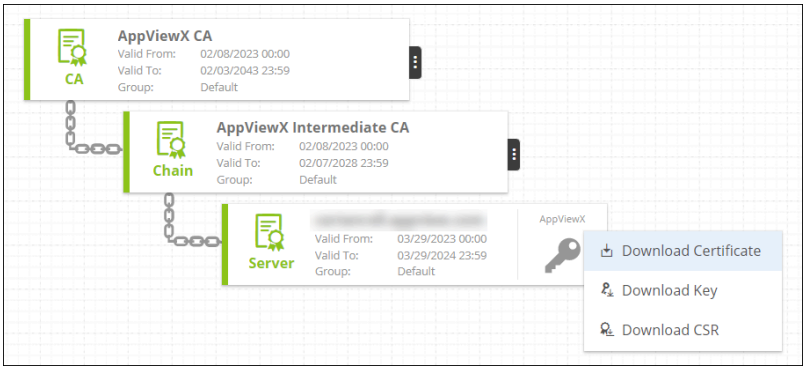
8. Under the **ServiceNow Details** section, enter the **RITM ticket Number** (mandatory).
9. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).

10. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.
11. Click **Submit**.
    AppViewX Certificate is created successfully and the RITM ticket status updated. The certificate is updated in the ServiceNow ticket.

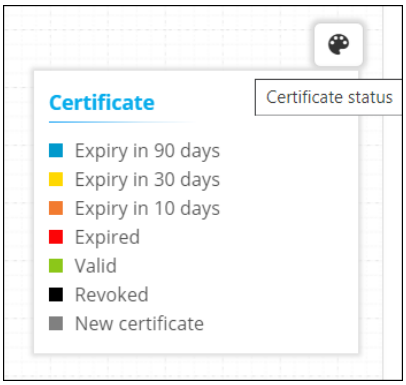
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



12. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



13. Hover your mouse over to view the **Certificate status**.



Enroll Certificate and Push with ServiceNow

This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM) and push it to the selected device.

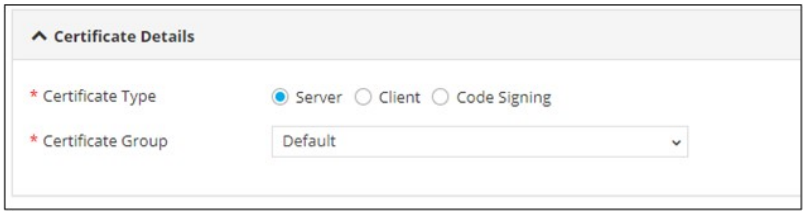
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push with ServiceNow** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.



Field description for Certificate Details section

Field	Description
***Certificate Profile**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*****) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when DigiCert or Entrust are selected as the CA.
Description	Provide a description of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully qualified domain name (FQDN) of the server for which the certificate is requested.

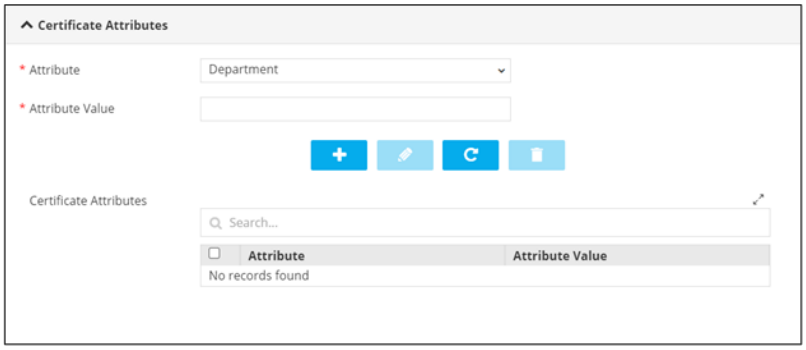
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subject Alternative Name (SAN)	Select the SAN as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
***Organization**	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Organization Address	Enter the address of the organization.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Email Address	Enter the email address
Locality	Enter the name of the locality in which the organization is situated.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** or • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options - RSA, DSA, EC.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the Hash Function from the available options.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Download Format**	Select the format for downloading the certificate from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.

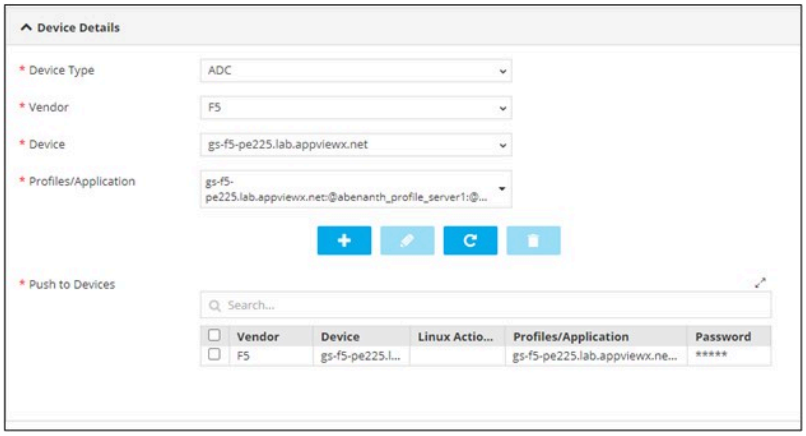


Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Device Details** section, select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



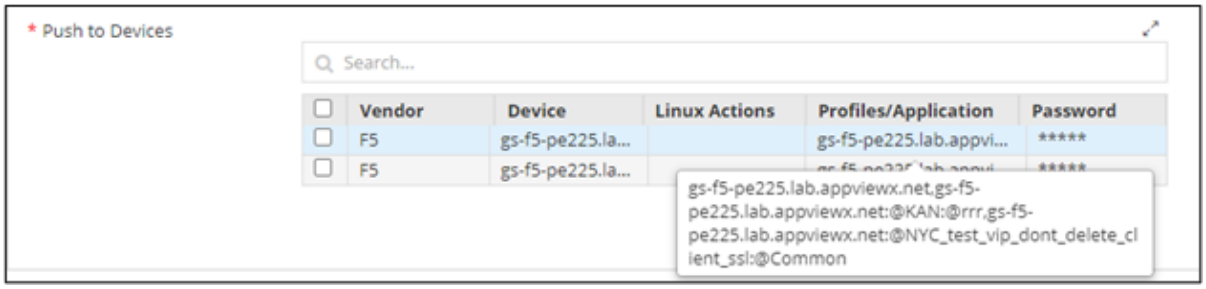
Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

8. To add the selected profile/application to the grid, click .
   The **Profile/Application** is added to the **Push to Devices** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



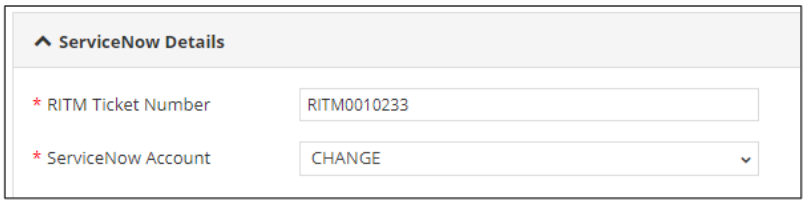
Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

9. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

Note: This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

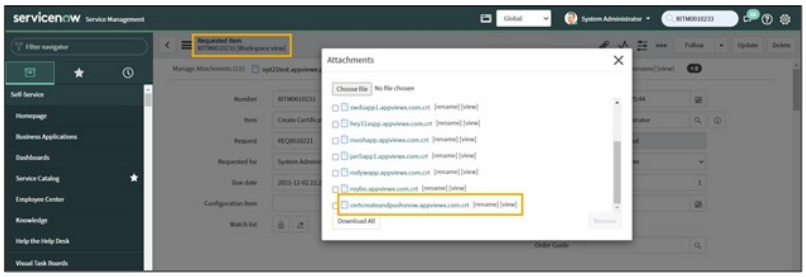
10. Under the **ServiceNow Details** section, enter the **RITM ticket Number** (mandatory).
11. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).



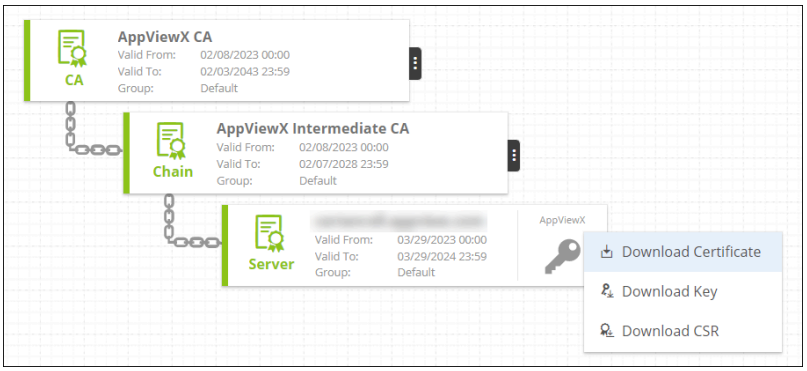
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.
13. Click **Submit**.

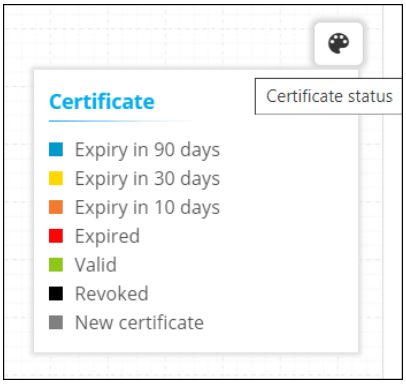
    AppViewX Certificate is created successfully and pushed to the selected device. RITM ticket status updated and the certificate updated in the ServiceNow ticket.



14. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



15. Hover your mouse over to view the **Certificate status**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Easy Certificate Provisioning

This workflow allows you to create an AppViewX certificate and push to a device available in the instance. Once the certificate is created, an email is sent to the logged in user informing them about the Push to Device Status of the certificate.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** window, under the **Enrollment** category, hover your mouse over the **Easy Certificate Provisioning** workflow and click .

   > **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CSR Parameters** section, enter the **Common Name**.

   > **Note:** This is a mandatory field.

3. Under the **CSR Parameters** section, enter the **Subject Alternative Name**.

4. Under the **Device Details** section, enter or select the requested field information as described in the table below.

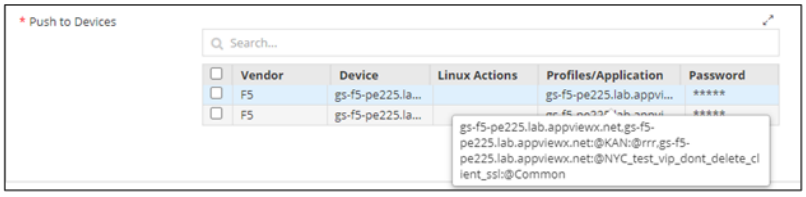
Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the Push to Devices grid, click +.
   The profile/application is added to the **Push to Devices** grid.



Note: If you select multiple profiles/applications, they will be displayed in the Push to Devices grid, under the **Profiles/Applications** column as comma-separated values.

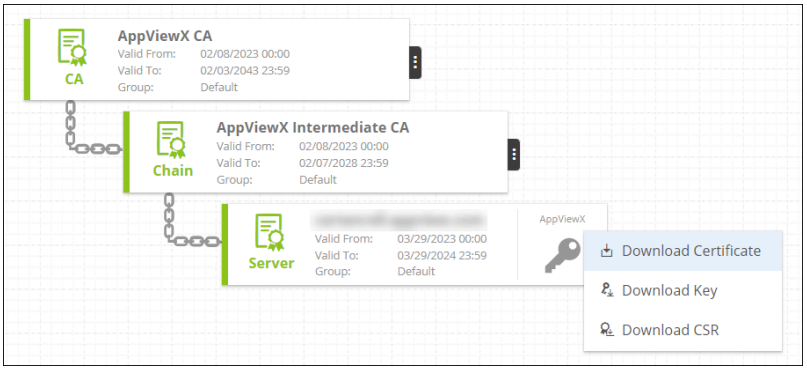
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

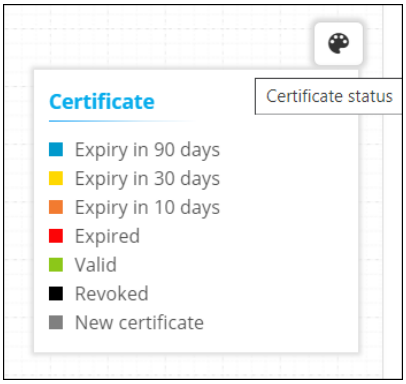
6. Click **Submit**.
   AppViewX certificate is created and pushed to the selected device. At the **Summary** stage of workflow execution, a Push to Device Status grid is displayed, which can be downloaded by clicking from the top right corner of the screen.

7. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. Hover your mouse over to view the Certificate status.



Enroll Certificate with CAA Validation

This workflow allows you to create a certificate by validating the Certificate Authority that can issue the certificate based on the given domain name.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with CAA Validation** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the requested field information as described in the table below.

Field description for Certificate Details section

Field	Description
***Certificate Category**	Select the required **Certificate Profile** from the available options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Group**	Select the required **Certificate Group** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

3. Under the **CA Details** section, enter or select the requested field information as described in the table below.

Field description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Enter a **Description** of the workflow, if required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
All asterisk (*) marked fields are mandatory.	

4. Under the **CSR Parameters** section, enter the field information as described in the table below.

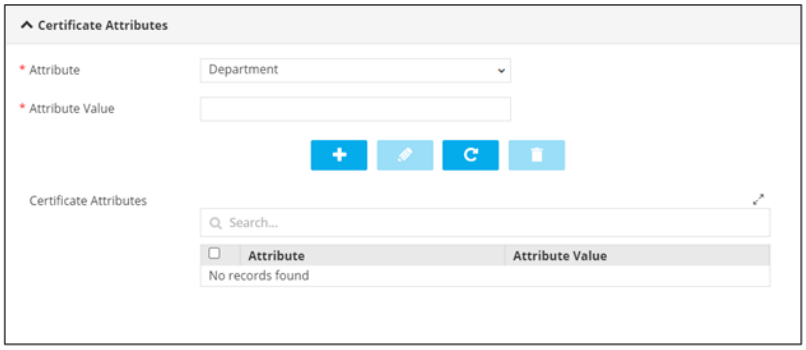
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization. **Note:** This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

5. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
6. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

7. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

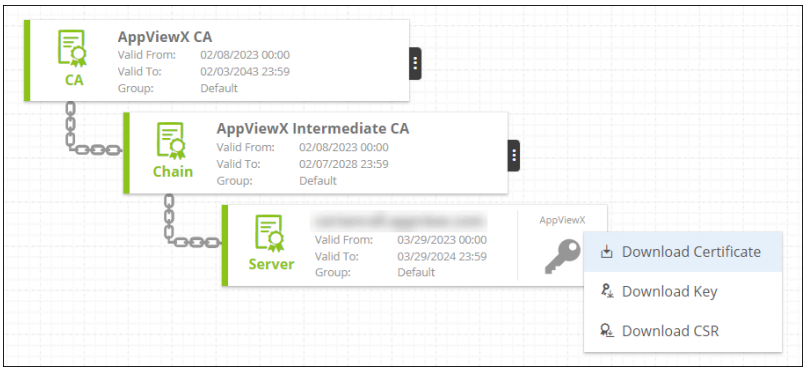
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

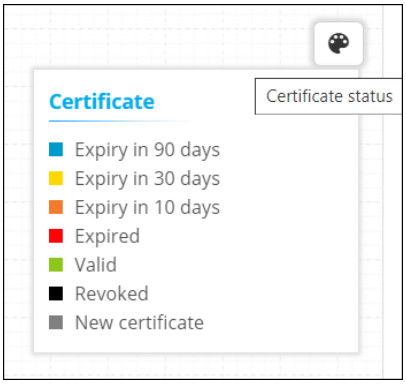
8. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

9. Click **Submit**.
   CAA Validation is successful and the certificate is created successfully.
10. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



11. Hover your mouse over to view the Certificate status.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enroll Certificate and Push

This workflow allows you to create a certificate and push it to the selected device.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push** workflow and click .
   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **CA Details** section, select the requested field information as described in the table below.

Field Description for CA Details section

Field	Description
***Certificate Profile**	Select the Certificate Profile from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
***Auto Regenerate**	Select the required radio button to enable/disable **Auto Regenerate**. **Note:** Default selection is set to **Off**.
Start Regenerating (Days)	Enter the number of days in the **Start Regenerating (days)** field. **Note:** This field is displayed only when the **Auto Regenerate** field is enabled.
***Input Method**	Select the required **Input Method**. The options available are: • **Manual**: (Default) If you select the **Input Method** as **Manual**, the CSR parameters will have to be entered/selected manually. For instructions, click here. • **Policy Based**: If you select the **Input Method** as **Policy Based**, the CSR parameter fields will be auto-populated based on the policy associated with the selected **Certificate Group**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	For instructions, click here. • **Upload CSR**: If you select the **Input Method** as **Upload CSR**, you can upload the CSR file to fetch the CSR parameters. For instructions, click here.
All Asterisk (*) marked fields are mandatory.	

Enrolling Certificates Based on Input Method

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under **CSR Parameters**, enter the requested field information as described in the table below.

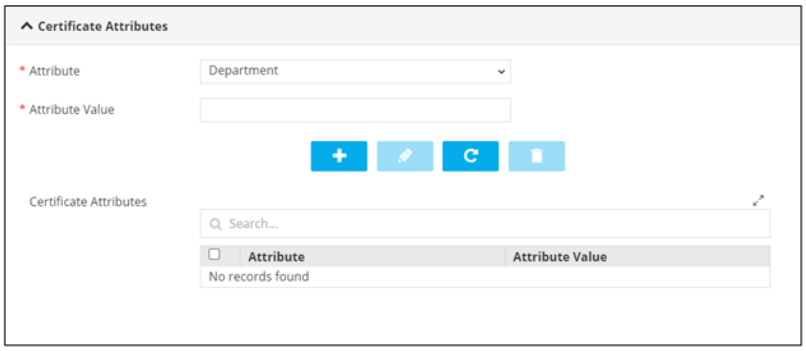
Field description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Email Address	Enter the email address associated with the **Certificate Group**.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Device Details** section, enter or select the requested field information as described in the table below.

Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.

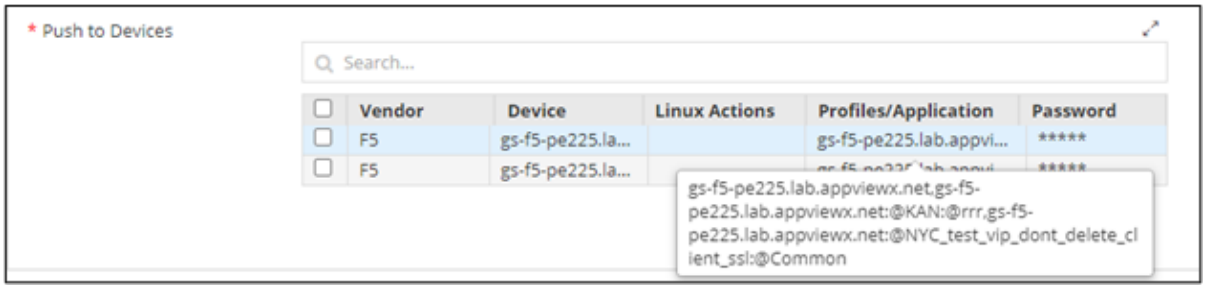
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the grid, click +.

   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

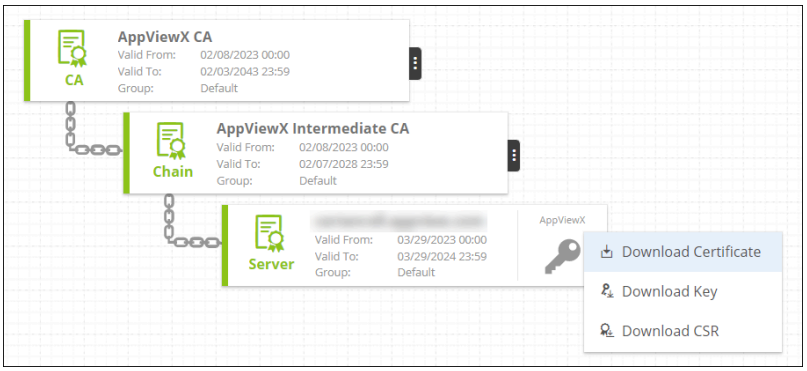
Action	Description
✎	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click ✎, enter the new value for the attribute, and click ✎ again.
🗑	Allows you to delete a profile/application.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

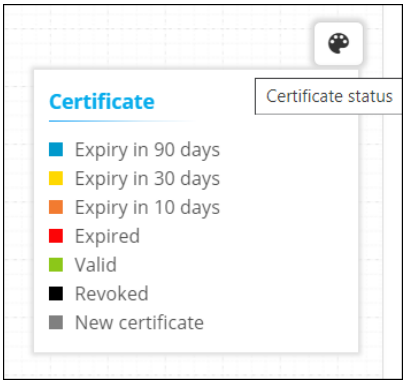
Action	Description
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

6. Click **Submit**.
   Certificate is created successfully and pushed to selected device.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



8. Hover your mouse over to view the **Certificate status**.



Policy Based

After you select the **Input Method** as **Policy Based**, execute the following steps to enroll a certificate:

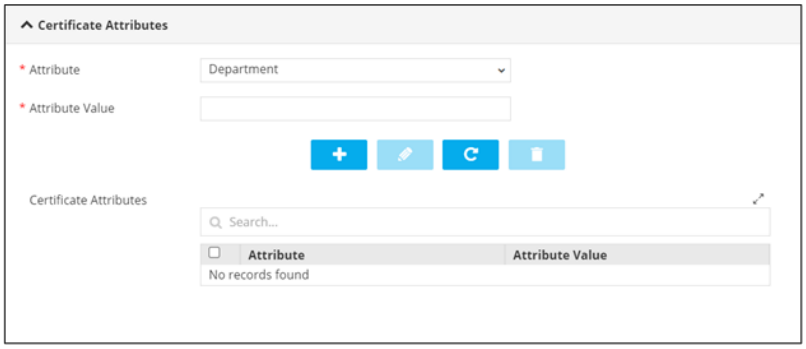
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Under the **CSR Parameters** section, enter the field information as described in the table below.

> **Note:** Some **CSR Parameters** will be auto-populated based on the policy associated with the **Certificate Group**.

> **Note:** For more information on the form fields, refer to the field information described in the Manual section.

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.
✎	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click ✎, enter the new value for the attribute, and click ✎ again.
🗑	Allows you to delete a certificate attribute.
⤢	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Device Details** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

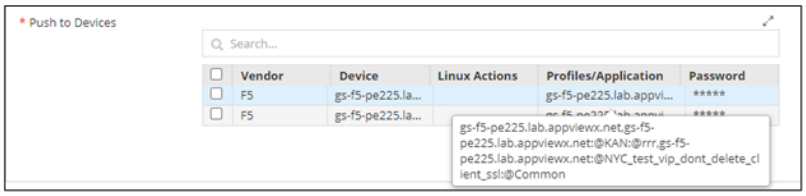
Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

5. To add the selected profile/application to the grid, click .
   The **Profile/Application** is added to the **Push to Devices** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.

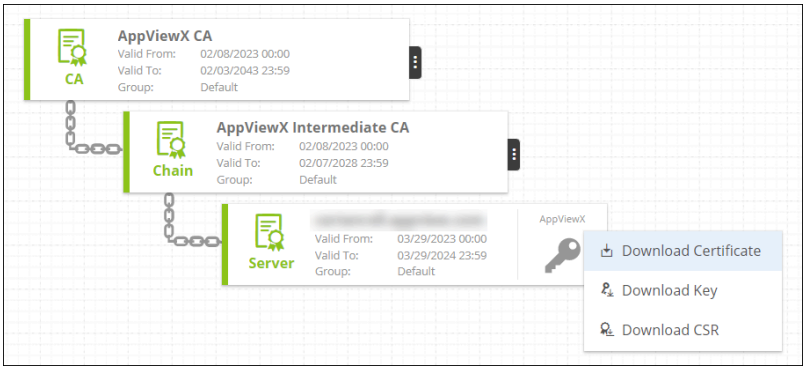


Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

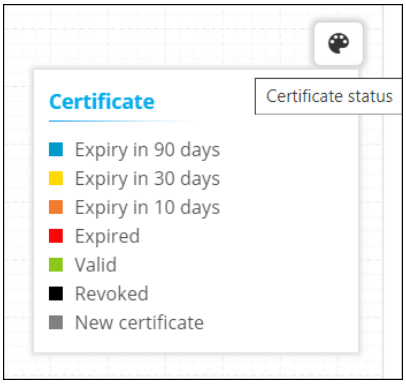
6. Click **Submit**.
   Certificate is created successfully and pushed to selected device.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

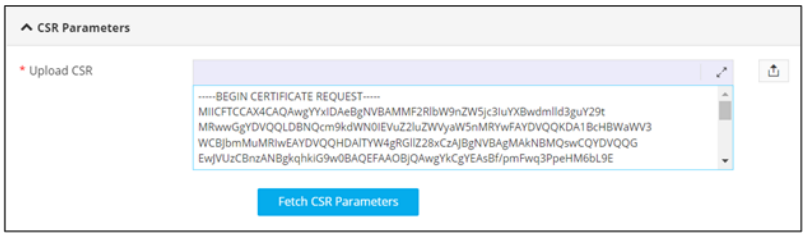
8. Hover your mouse over to view the **Certificate status**.



Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click .

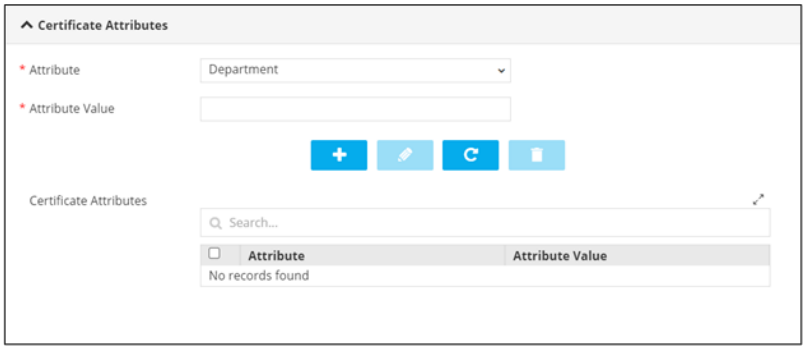


2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Policy Based section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

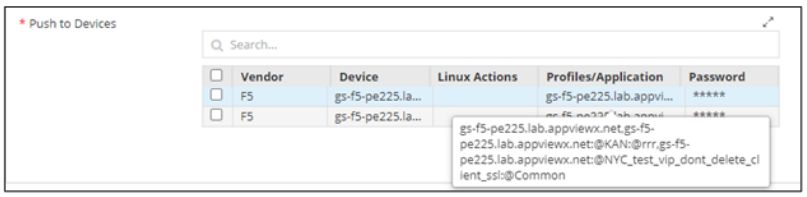


Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. To add the selected profile/application to the grid, click .
   The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

6. Under the **Device Details** section, enter or select the requested field information as described in the table below.

Field description for Device Details section

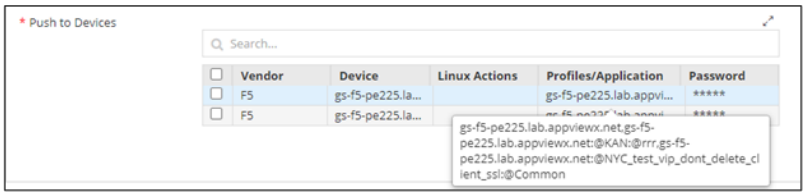
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

7. To add the selected profile/application to the grid, click .
   The **Profile/Application** is added to the **Push to Devices** grid.

   Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



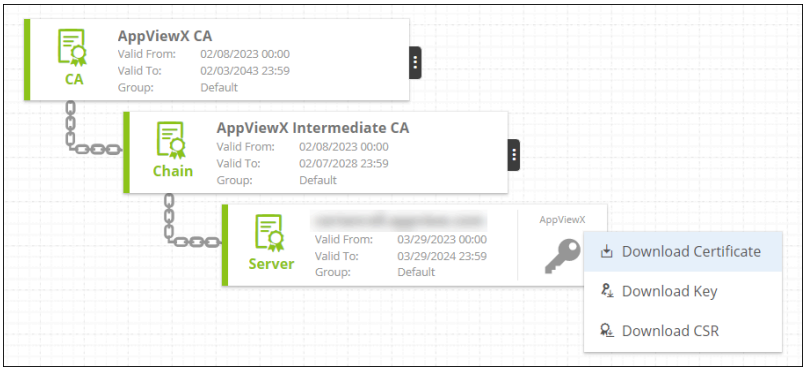
Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

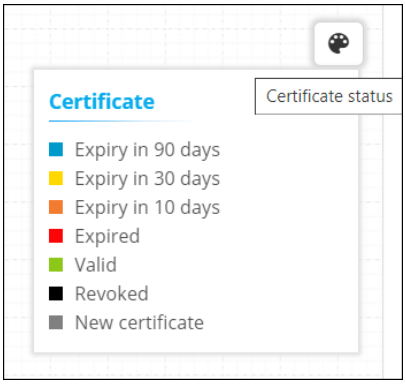
8. Click **Submit**.
   Certificate is created successfully and pushed to selected device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



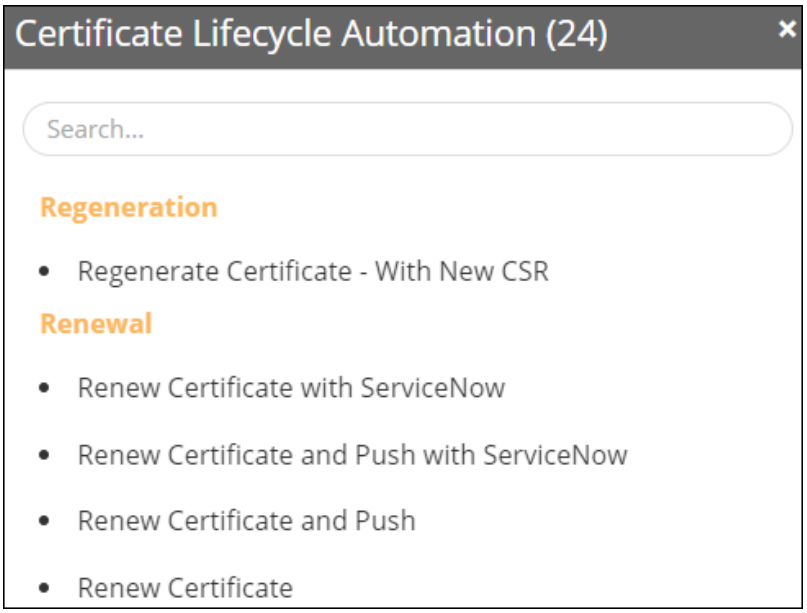
10. Hover your mouse over to view the **Certificate status**.



Renew Certificate Workflows

This section lists and describes the workflows that can be used to renew and regenerate certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Renewal with Incident Automation. These workflows are available in the **Certificate Lifecycle Automation** catalog under the **Regeneration** and **Renewal** categories.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- Renew Certificate
- Regenerate Certificate with New CSR
- Renew Certificate and Push
- Renew Certificate with ServiceNow
- Renew Certificate and Push with ServiceNow

Renew Certificate

This workflow allows you to renew a certificate based on the certificate group and certificate authority.

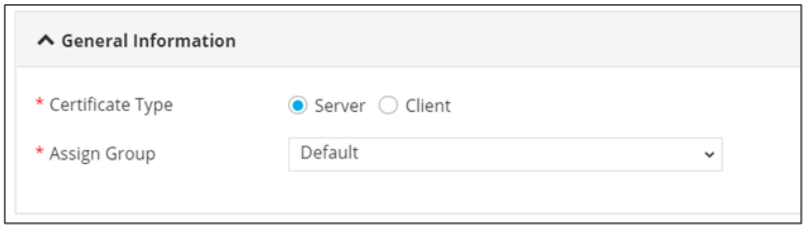
To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate** workflow and click .

   > **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).
5. Under the **CA Details** section, add a description for the certificate being renewed (optional).

6. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.
7. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

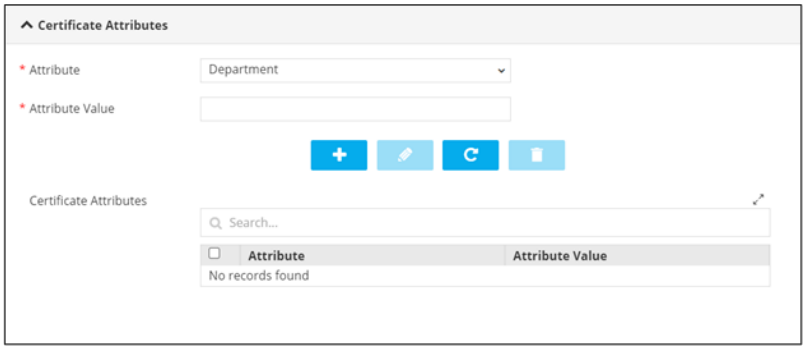
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which the certificate is requested.
Subject Alternative Name (SAN)	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code of the organization.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
***Validity Unit**	Select the validity unit as: • **Days** • **Months** • **Years**
***Validity Value**	Select a valid validity value.
***Key Type**	Select a **Key Type** from the available options.
***Bit Length**	Select the **Bit Length** from the available options. The values displayed in the dropdown will differ depending on the **Key Type** selected.
***Hash Function**	Select the **Hash Function** from the available options.
All Asterisk (*) marked fields are mandatory.	

8. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
9. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

10. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert, EJBCA, or Entrust is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

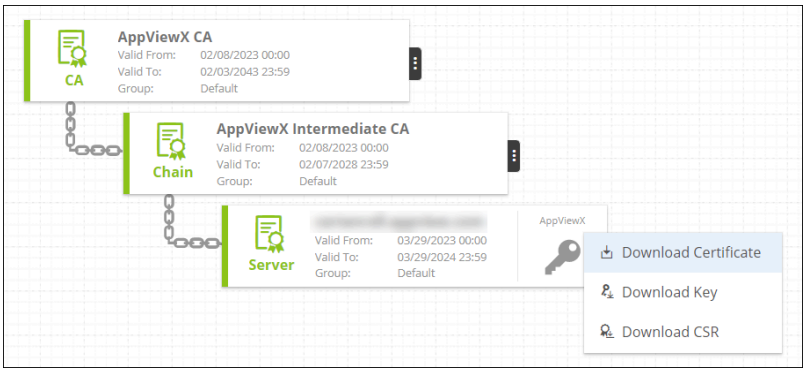
11. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

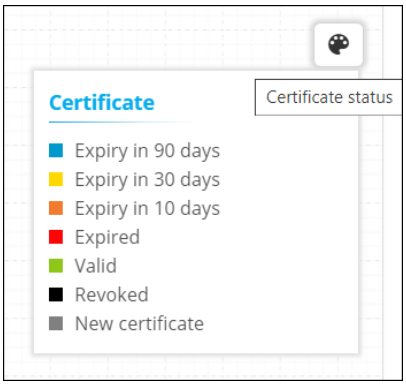
12. Click **Submit**.
    Certificate is renewed successfully.

13. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



14. Hover your mouse over to view the Certificate status.



Regenerate Certificate with New CSR

This workflow allows you to regenerate a certificate with a new CSR.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Regenerate Certificate with New CSR** workflow and click .

   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **Certificate Details** section, select the **Certificate Type** (mandatory).
3. Under the **Certificate Details** section, select the **Assign Group** (mandatory).
4. Under the **CA Details** section, enter or select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for CA Details section

Field	Description
***Certificate Authority**	Select the **Certificate Authority** from the available options: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This list will be populated based on the **Certificate Group** selected in the **Certificate Details** section.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the CA selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when Digicert is selected as the CA.
***Cert Type**	Select the **Cert Type** from the options available in the dropdown. **Note:** This field is displayed only when Digicert or Entrust are selected as the CA.
Description	Enter a **Description** of the workflow, if required.
All asterisk (*) marked fields are mandatory.	

What to do next:

- For steps to enroll a certificate based on **Input Method** - **Manual**, click here.
- For steps to enroll a certificate based on **Input Method** - **Upload CSR**, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Manual
- Upload CSR

Manual

After you select the **Input Method** as **Manual**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

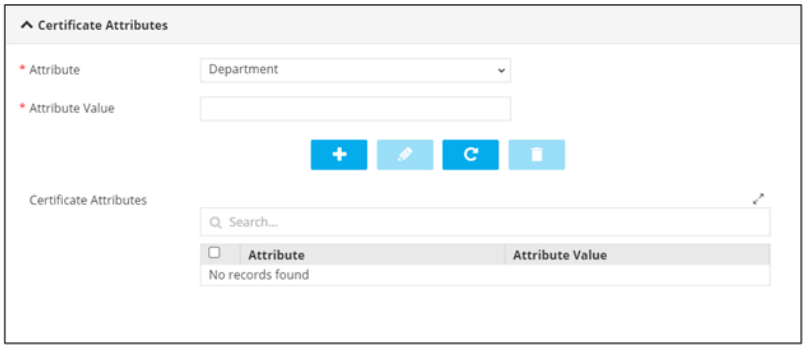
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate **Note:** You have the option to change the common name of the regenerated
Subject Alternative Name	Select the **SAN** as either: • **Directory Name** • **Email** • **Registered ID** • **URL** • **Other Name** • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN**
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated
Locality	Enter the name of the locality in which the organization is situated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code.
Email Address	Enter the email address associated with the **Certificate Group**.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

2. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
3. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

4. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

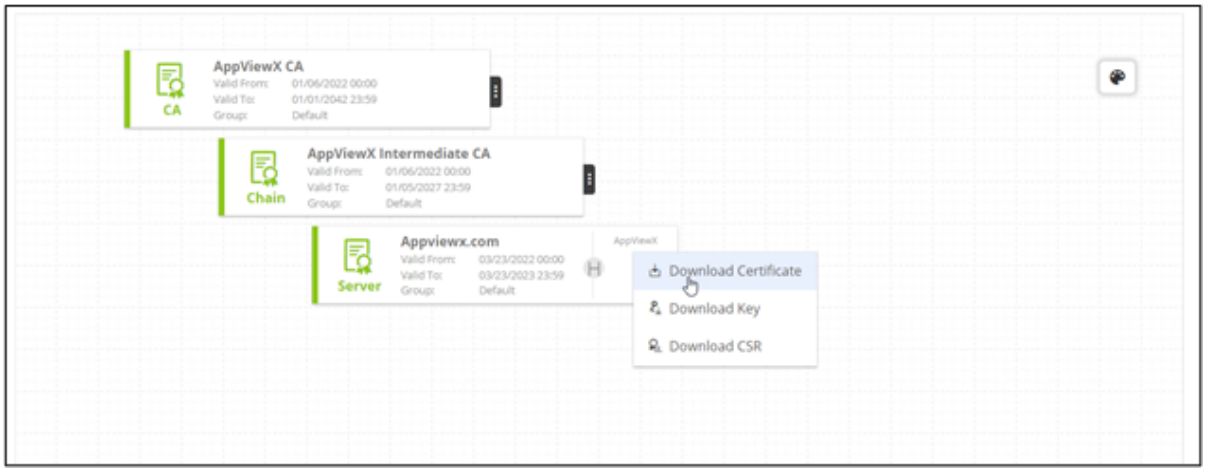
5. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

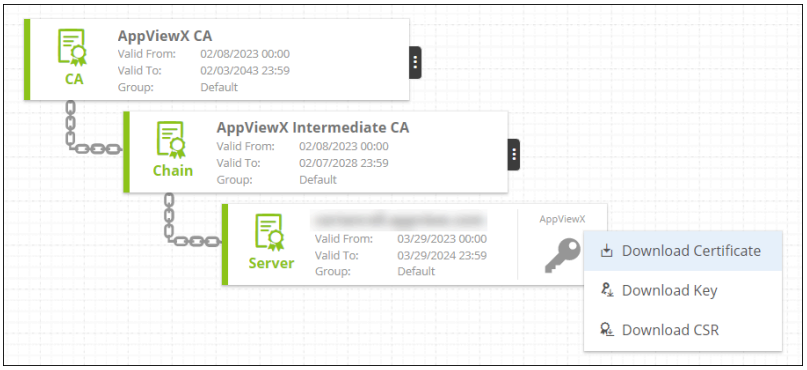
6. Click **Submit**.
   Certificate is regenerated successfully.

7. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

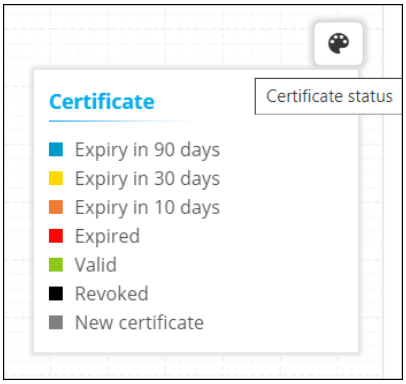
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



8. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



9. Hover your mouse over to view the Certificate status.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

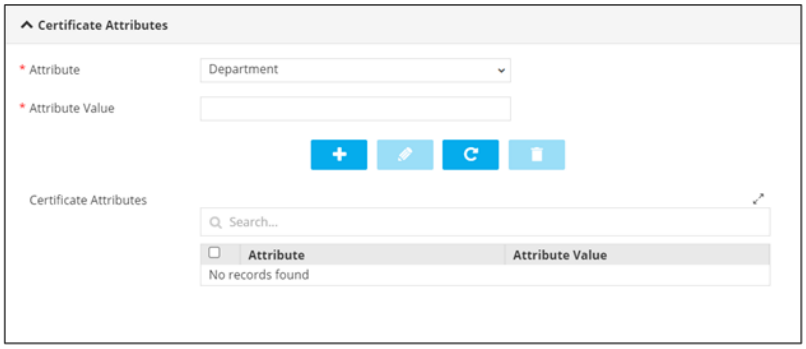
Upload CSR

After you select the **Input Method** as **Upload CSR**, execute the following steps to enroll a certificate:

1. Under the **CSR Parameters** section, to **Upload CSR**, click .
2. Click **Fetch CSR Parameters**.

> **Note:** Some CSR parameters are fetched from the uploaded CSR file. For more information on the remaining form fields, refer to the field information described in the Manual section.

3. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
4. Enter a value for the selected attribute.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

5. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** This section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

6. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

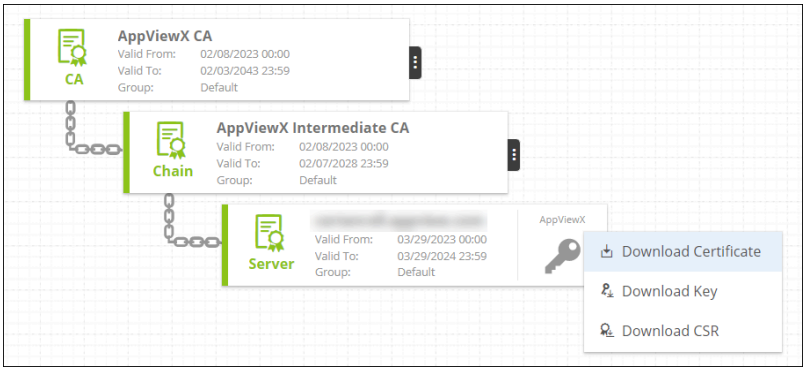
> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

7. Click **Submit**.
   Certificate is regenerated successfully.

8. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



Renew Certificate and Push

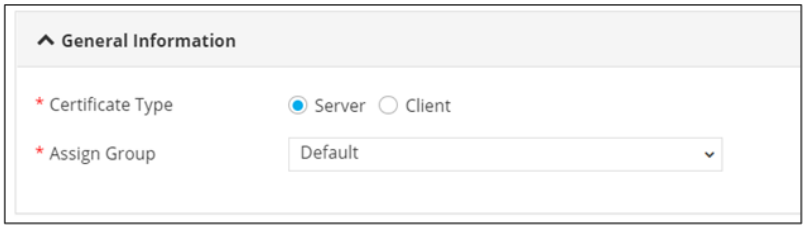
This workflow allows you to renew a certificate based on the certificate group and certificate authority and push it to the selected device.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate and Push** workflow and click .

> **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).



4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).
5. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** and **CA Account** fields are populated based on the Certificate selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

Field Description for CSR Parameters section

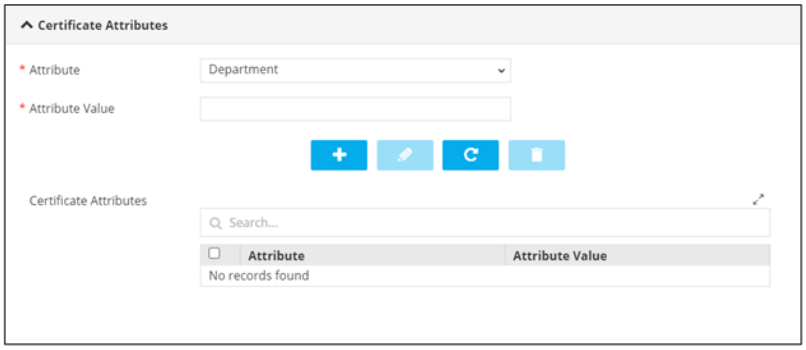
Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **Directory Name** • **Email** • **Registered ID** • **URL** • **Other Name** • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Email Address	Enter a valid URL if you select the **URL** option in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
Country	Enter the name of the country in which the organization is located.
State	Enter the name of the state in which the organization is located.
Zip Code	Enter the zip code.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
All asterisk (*) marked fields are mandatory.	

7. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
8. Enter a value for the selected attribute.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

9. Under the **Vendor Specific Details** section, select the field information from the options available in the dropdown.

> **Note:** This section is displayed only when DigiCert, EJBCA, or Entrust is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

10. Under the **Device Information** section, select the field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

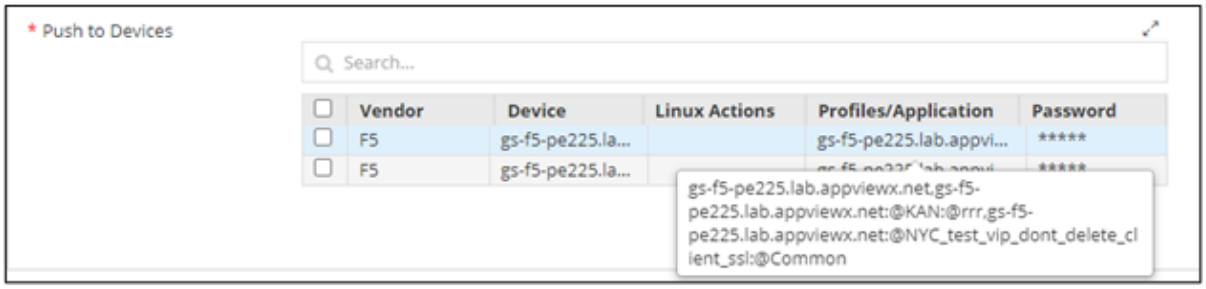
Field description for Device Details section

Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
Vendor	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
Device	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

11. To add the selected profile/application to the grid, click .
    The **Profile/Application** is added to the **Push to Devices** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

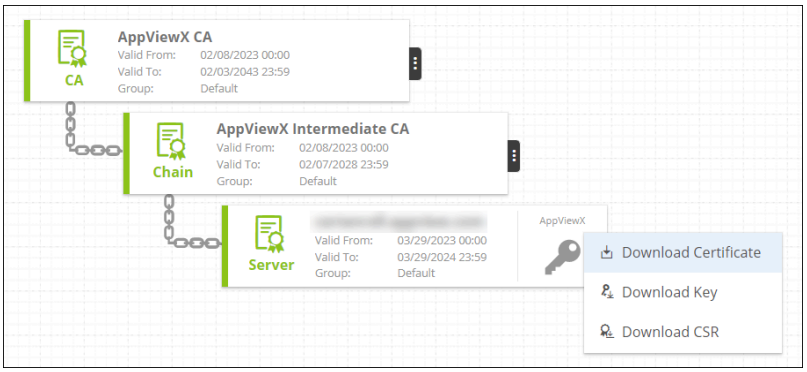
12. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

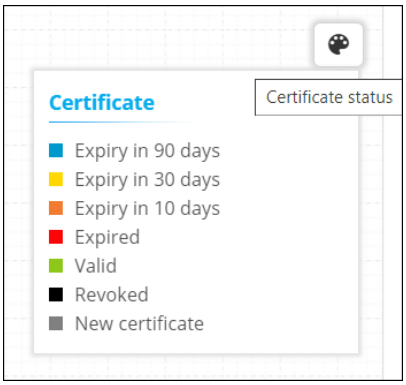
13. Click **Submit**.
    Certificate is renewed successfully.

14. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



15. Hover your mouse over to view the **Certificate status**.



Renew Certificate with ServiceNow

This workflow allows you to renew a certificate based on the certificate group and certificate authority and attach the renewed certificate to the ServiceNow ticket.

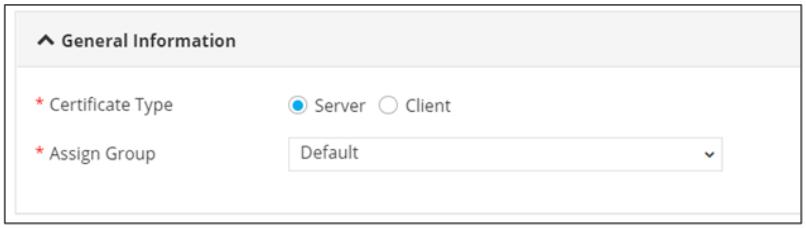
To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate with ServiceNow** workflow and click .

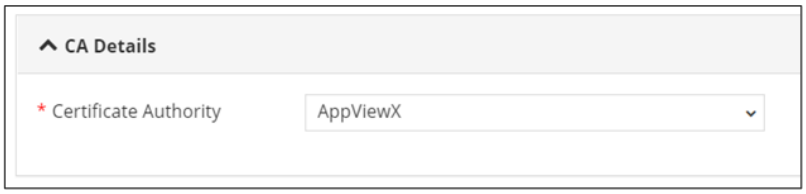
   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).

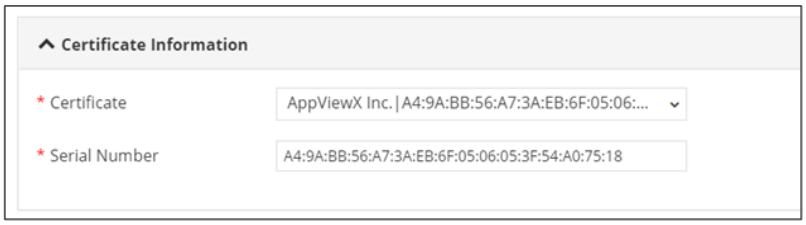
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).



5. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.



6. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

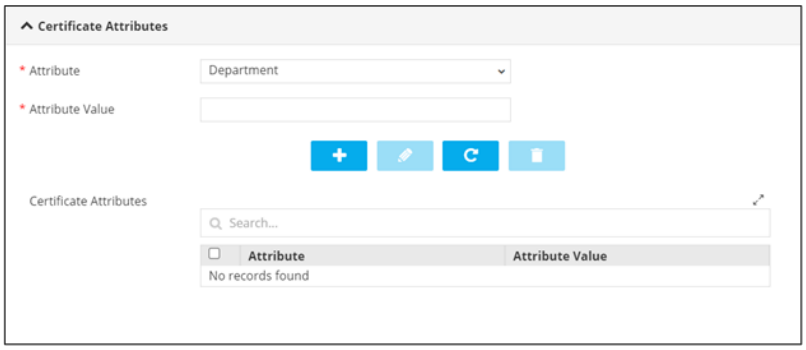
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **Directory Name** • **Email** • **IP Address** • **Registered ID**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **URL** • **Other Name**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Validity Unit	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
Validity Value	Enter a **Validity Value** based on the selected validity unit.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Download Format**	Select the format for downloading the certificate from the available options.
All asterisk (*) marked fields are mandatory.	

7. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
8. Enter a value for the selected attribute.

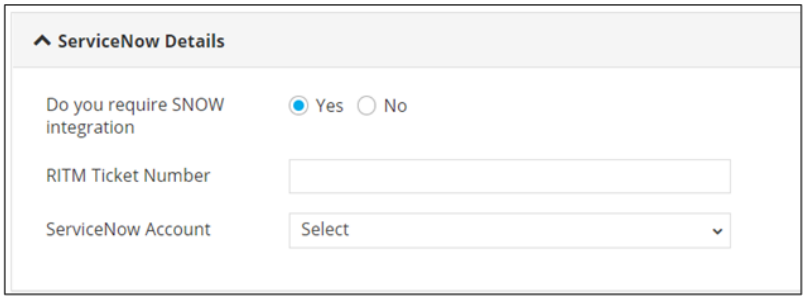


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions available in the Certificate Attributes grid

Action	Description
	Allows you to add the attribute to the **Certificate Attributes** grid.
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

9. Under the **ServiceNow Details** section, enter or select the requested field information as described in the table below.



Field Description for ServiceNow Details section

Field	Description
Do you require SNOW Integration?	Select the required radio button for ServiceNow integration.
RITM Ticket Number	Enter the RITM Ticket Number to which the downloaded certificate will be attached. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.
ServiceNow Account	Select the ServiceNow Account from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

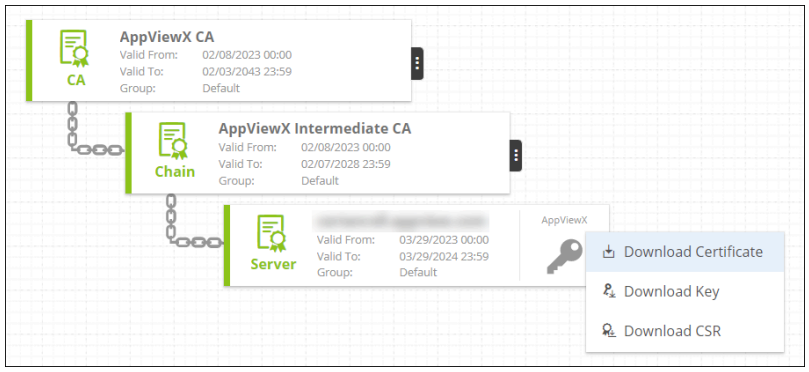
Field	Description
	Note: This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.

10. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

    Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

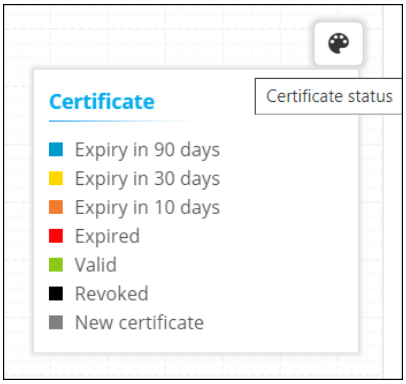
11. Click **Submit**.
    Certificate is renewed successfully.

12. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

13. Hover your mouse over to view the **Certificate status**.



Renew Certificate and Push with ServiceNow

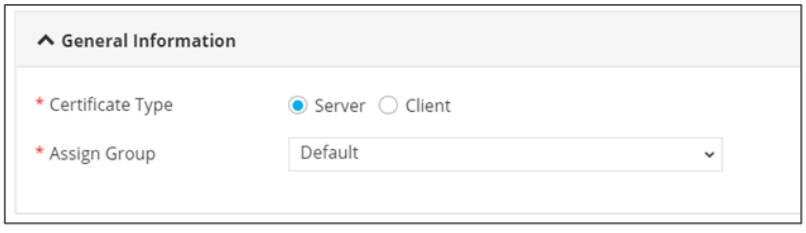
This workflow allows you to renew a certificate based on the certificate group and certificate authority, push it to a device, and attach the renewed certificate to the ServiceNow ticket.

To trigger this workflow:

1. From the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate and Push with ServiceNow** workflow and click .

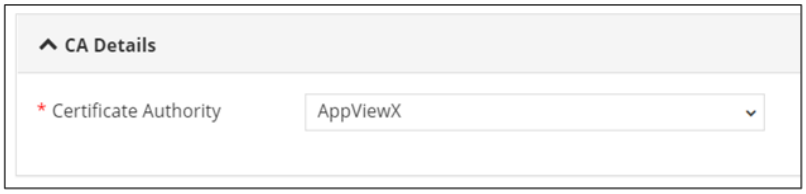
   Tip: You can also search for the workflow by typing the workflow name in the search bar.

   The workflow execution page is displayed with the workflow inputs requested at the first stage.
2. Under the **General Information** section, select the **Certificate Type** (mandatory).
3. Under the **General Information** section, select the **Assign Group** (mandatory).



4. Under the **CA Details** section, select the **Certificate Authority** (mandatory).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. Under the **Certificate Information** section, select the **Certificate** from the dropdown list (mandatory). The **Serial Number** field is populated based on the Certificate selected.

6. Under the **CSR Parameters** section, enter or select the requested field information as described in the table below.

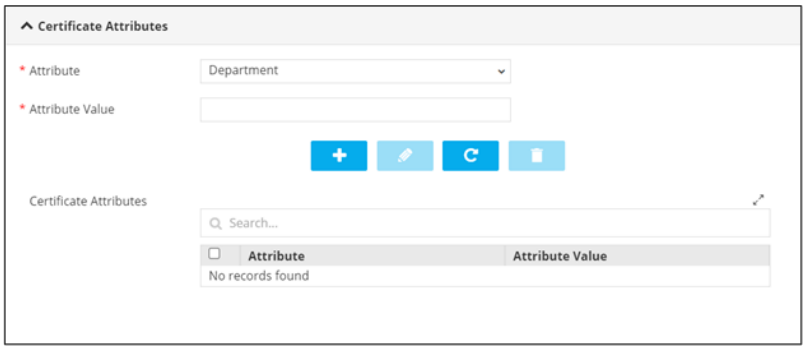
Field Description for CSR Parameters section

Field	Description
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested. **Note:** You have the option to change the common name of the regenerated certificate.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **Directory Name** • **Email** • **IP Address** • **Registered ID** • **URL** • **Other Name**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
Directory Name	Enter a valid Directory Name if you select the **Directory Name** option in the **SAN** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Registered ID	Enter a valid Registered ID if you select the **Registered ID** option in the **SAN** field.
Other Name	Enter a valid Other Name if you select the **Other Name** option in the **SAN** field.
URL	Enter a valid URL if you select the **URL** option in the **SAN** field.
Email	Enter a valid Email address if you select the **Email** option in the **SAN** field.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
***Download Format**	Select the format for downloading the certificate from the available options.
All asterisk (*) marked fields are mandatory.	

7. Under the **Certificate Attributes** section, select the **Attribute** from the available options.
8. Enter a value for the selected attribute.



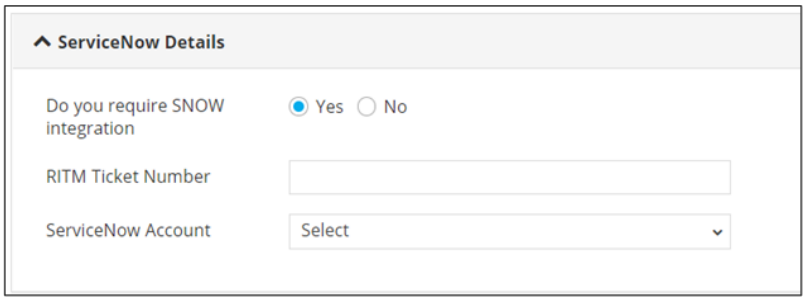
Actions available in the Certificate Attributes grid

Action	Description
+	Allows you to add the attribute to the **Certificate Attributes** grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Action	Description
	Allows you to edit the value of a particular attribute. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a certificate attribute.
	Allows you to maximize the **Certificate Attributes** grid.
Search bar	Allows you to search for a particular attribute in the grid.

9. Under the **ServiceNow Details** section, enter the requested field information as described in the table below.



Field Description for ServiceNow Details section

Field	Description
Do you require SNOW Integration?	Select the required radio button for ServiceNow integration.
RITM Ticket Number	Enter the RITM Ticket Number to which the downloaded certificate will be attached. **Note:** This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.
ServiceNow Account	Select the ServiceNow Account from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

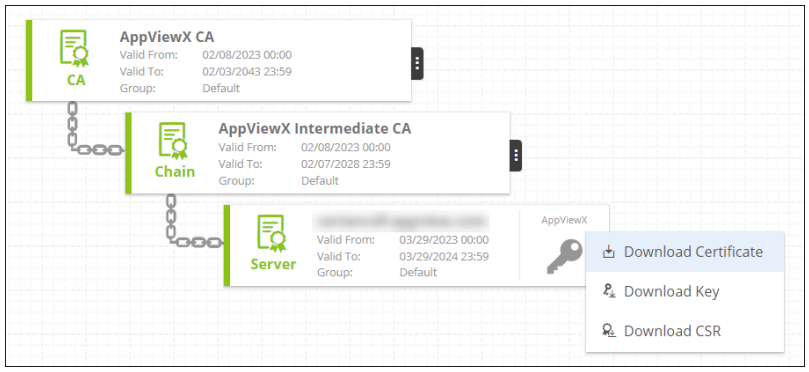
Field	Description
	Note: This field is displayed only when you select Yes in the **Do you require SNOW Integration?** field.

10. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

> **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

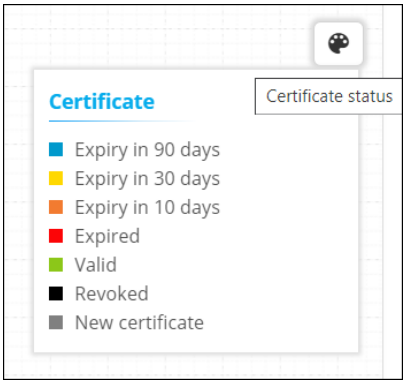
11. Click **Submit**.
    Certificate is renewed successfully.

12. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

13. Hover your mouse over to view the **Certificate status**.



Automation Workflow Tasks

- Overview
- Expiry Task
- Enrollment Tasks
- Renew Tasks
- Push Tasks

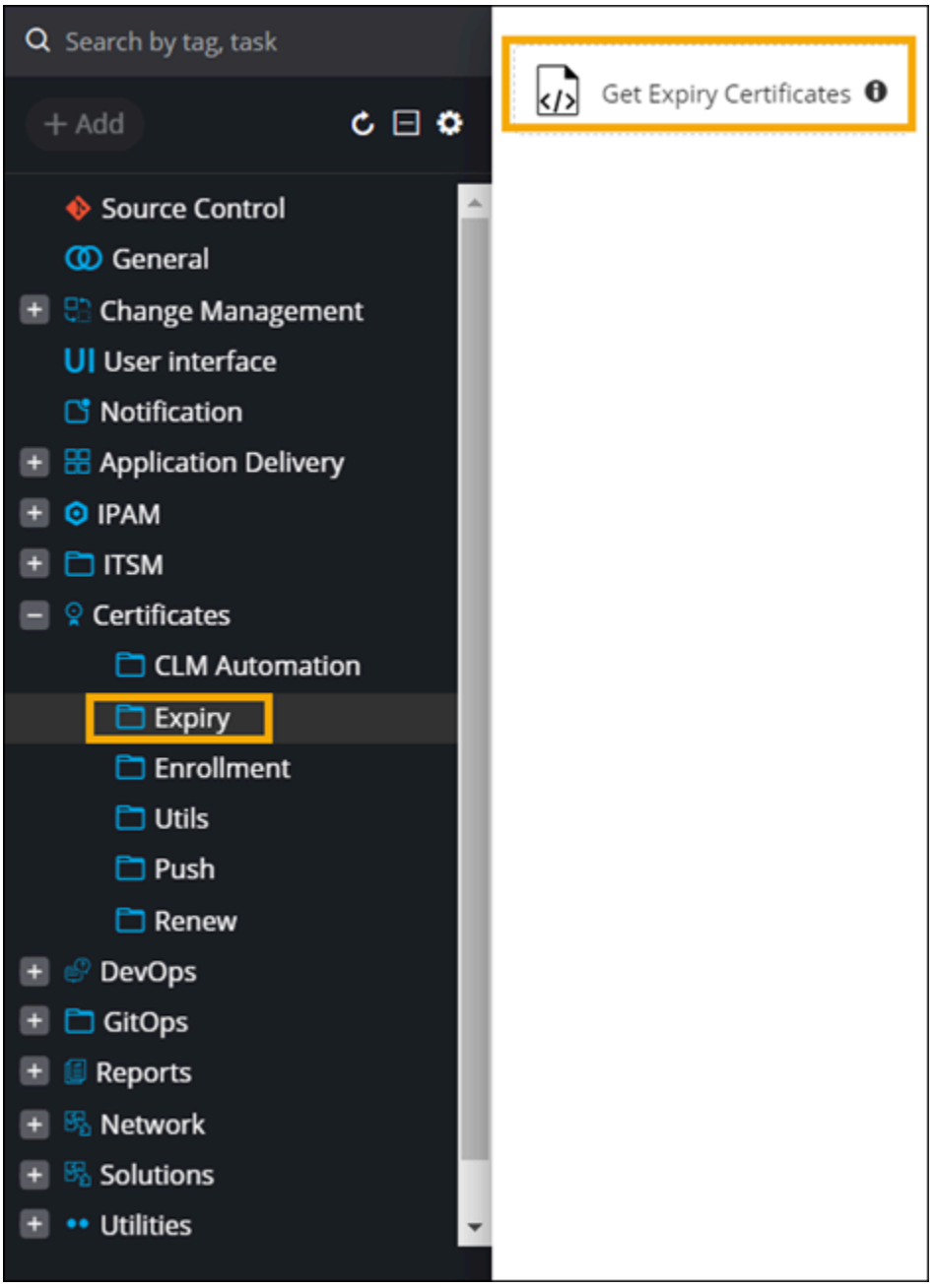
Overview

This section will describe the various OOB tasks available in the Workflow Studio.

Expiry Task

You can design a custom workflow for receiving certificate expiry notifications using the prebuilt task for getting expiry certificates available in the **Automation** module. The OOB script task for getting expiry certificates can be found under **Certificates** in the **Expiry** folder.

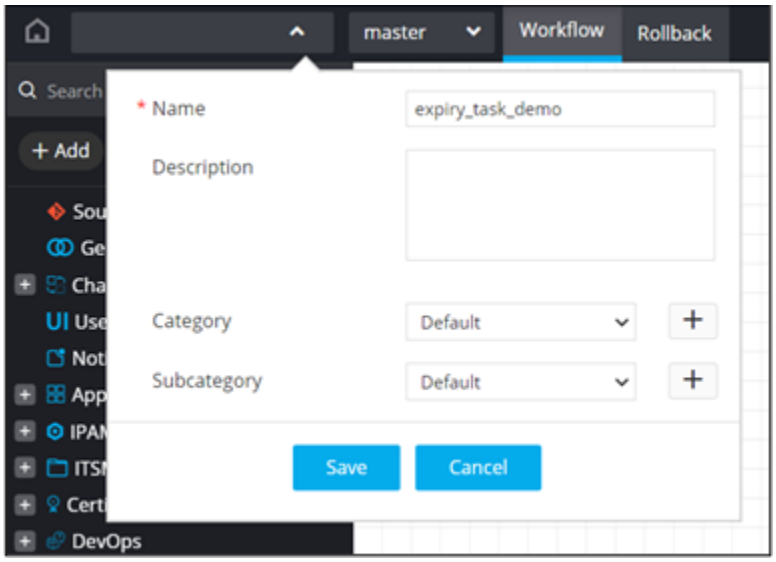
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



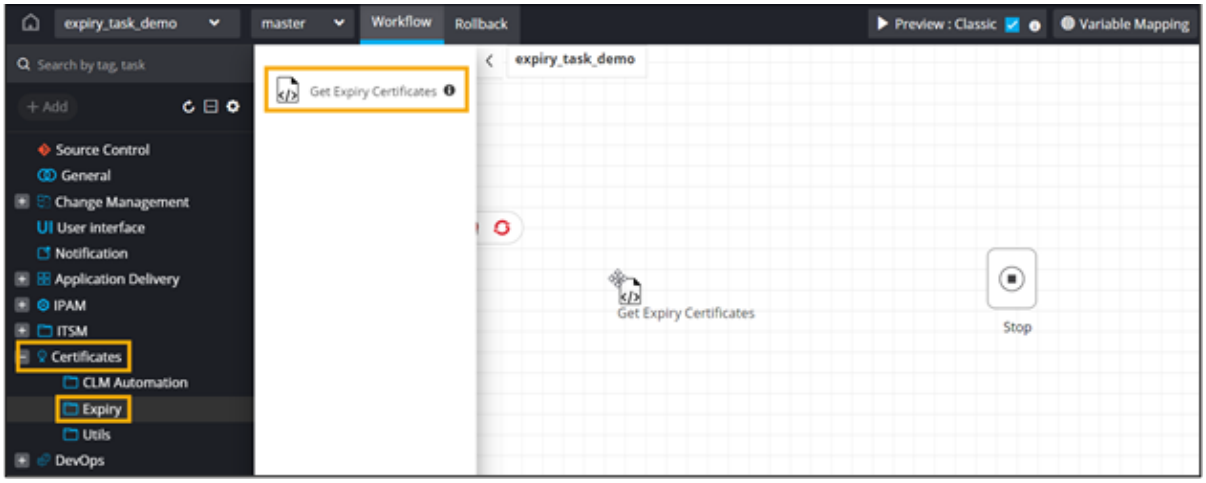
To design a custom workflow using the **Get Expiry Certificates** task

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

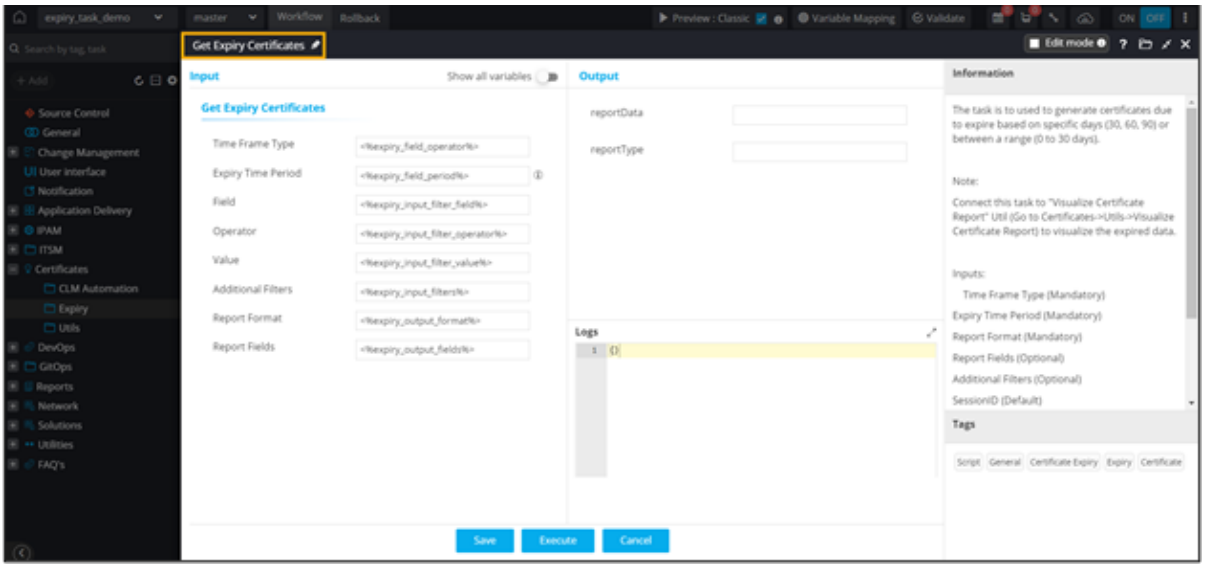


3. From the **Certificates**folder in the left menu, under **Expiry**, drag and drop the **Get Expiry Certificates** task.

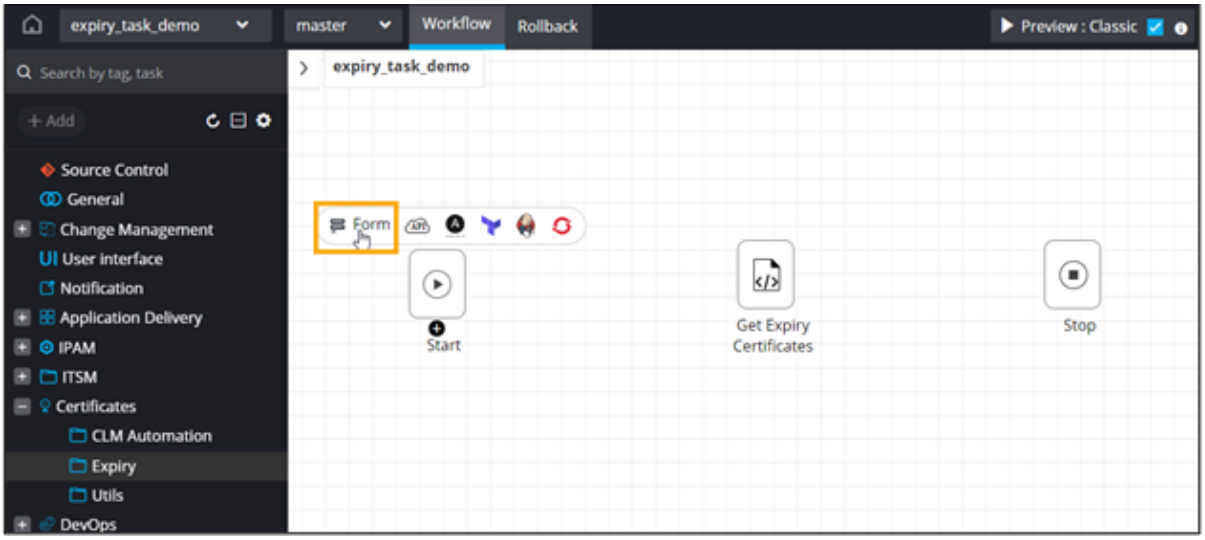


This task can be used to generate a report listing certificates due to expire in a specific number of days.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

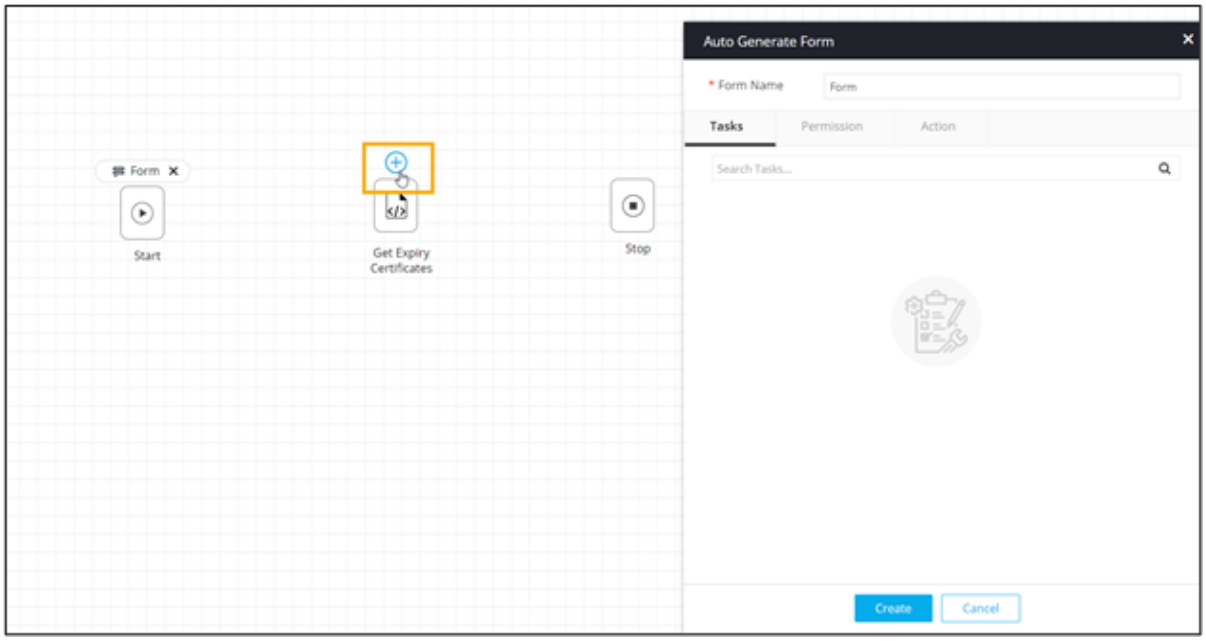


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.



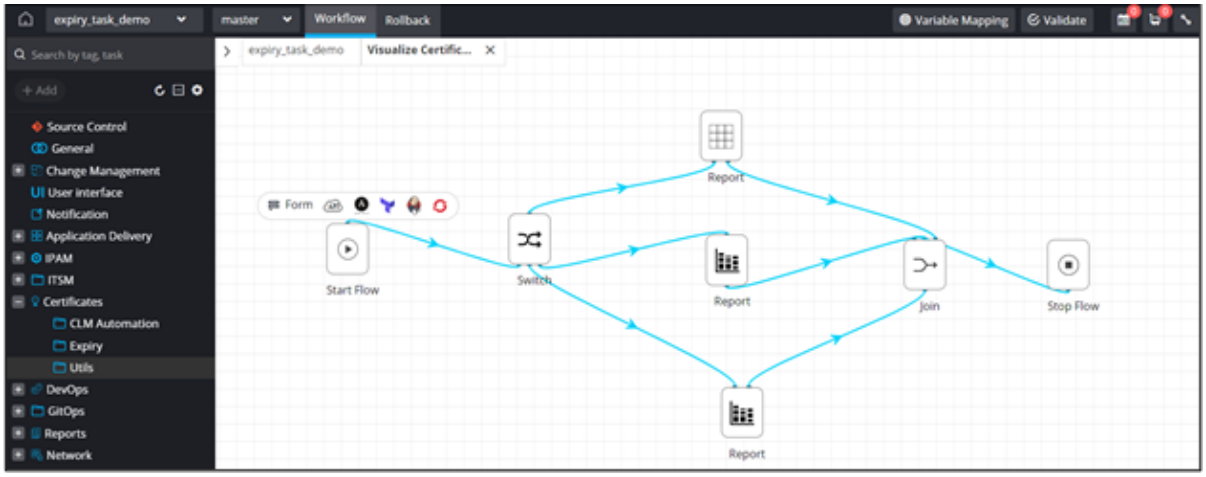
5. Click ⊕ above the **Get Expiry Certificates** task to auto-populate the form fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Enter a **Form Name** and click **Create**.
8. To display the certificate data in a report, from the **Utils** folder, drag and drop the **Visualize Certificate Expiry Report** prebuilt subflow.

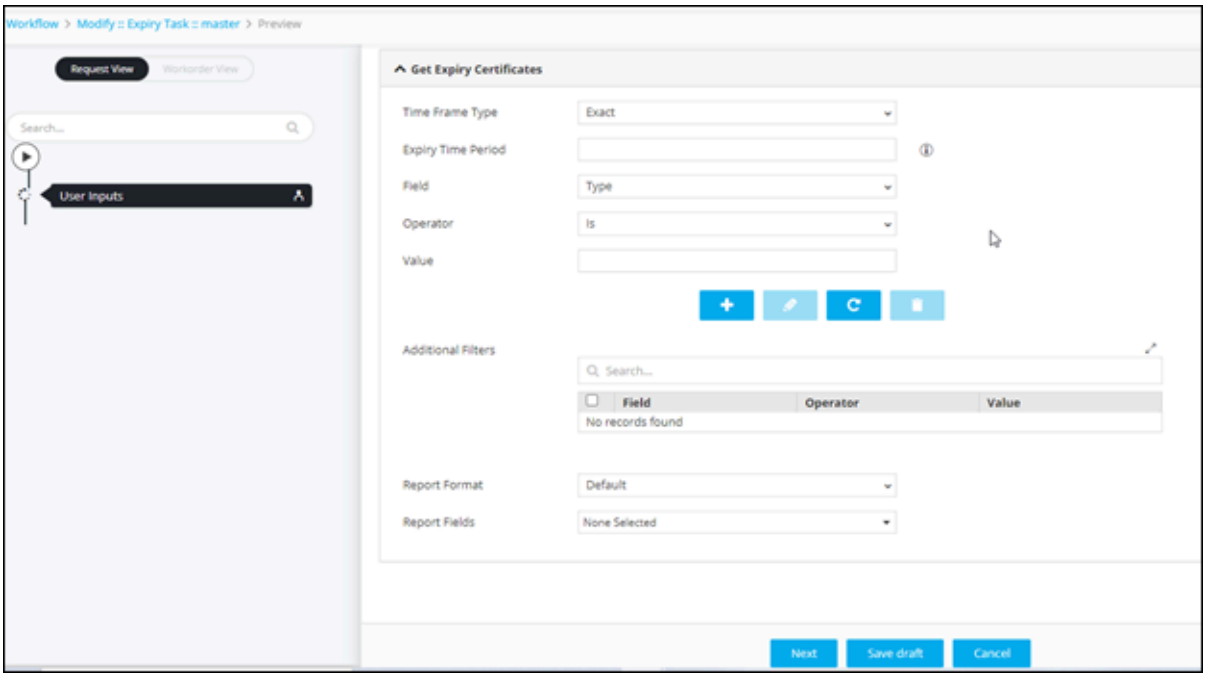
   This subflow includes **User Interface** tasks such as **Grid** and **Chart** (Pie chart and Stacked bar chart). The report generated will be displayed as a grid or a chart based on the inputs provided in the input form.



9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

   User Inputs form is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field Description for User Inputs form

Field	Description
Time Frame Type	Enter the time frame type from the available options: • **Exact** - Allows you to enter the exact value for the expiry time period (30 days). • **Range** - Allows you to give a range for the expiry time period (0 - 30). **Note: Exact** is the default selection.
Expiry Time Period	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Field	Select the field from the options available in the dropdown.
Operator	Select the conditional operator: • **Is** • **Is Not**
Value	Enter a valid value for filtering the certificates.

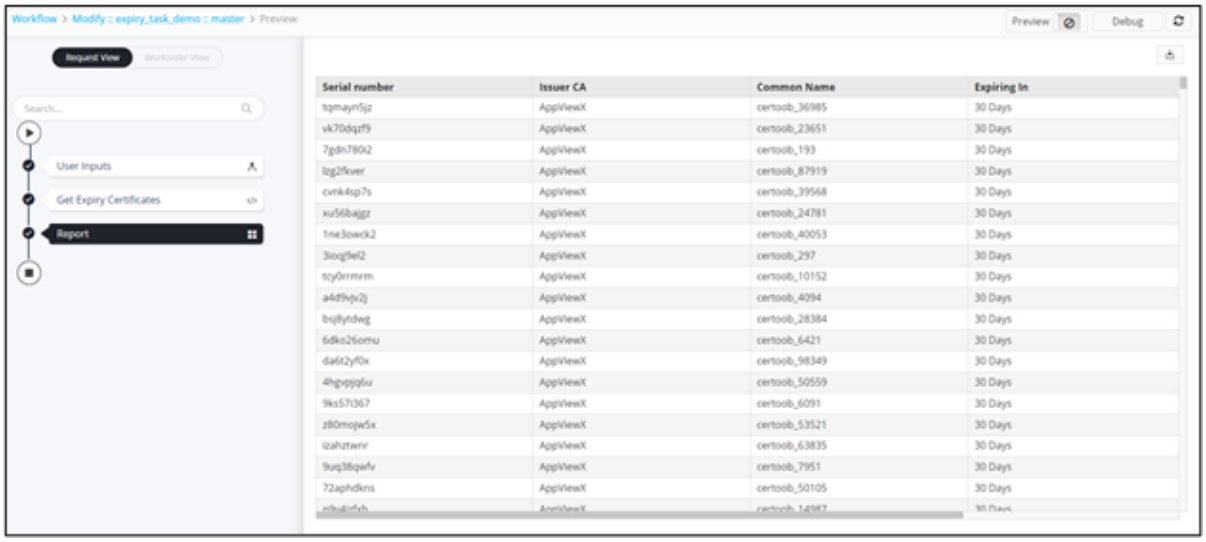
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Additional Filters	This grid displays the values selected in these fields: • **Field** • **Operator** • **Value** **Note:** The steps to apply these additional filters are given below the table.
Report Format	Select the format in which the report is displayed from the available options: • **Default** • **Pie Bar Chart** • **Stacked/Bar Chart**
Report Fields	Select the fields to be displayed in the report from the options available in the dropdown.

10. To add filters to the **Additional Filters** grid, click
11. To edit the value of a particular filter, select the filter in the grid and click .
12. Enter the new value(s) for the filters (Field/Operator/Value) and click again to update the value(s).
13. To delete a filter, select the filter in the grid and click .
14. To maximize the **Additional Filters** grid, from the top right corner of the grid, click .
15. Click **Next**.

    Report is generated with expiry certificates data displayed in Grid format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

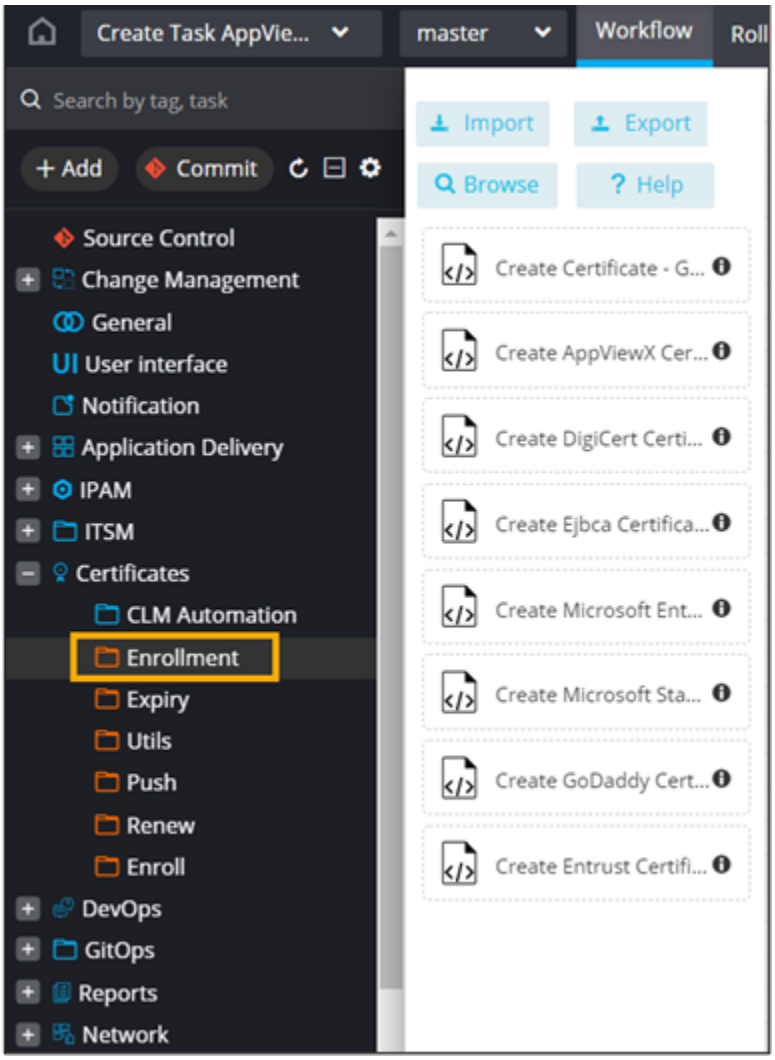


Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Enrollment Tasks

You can design a custom workflow for enrolling a certificate using the prebuilt Create Certificate tasks available in the **Workflow Studio**. The OOB script task for enrolling certificates through different Certificate Authorities can be found under **Certificates**, in the **Enrollment** folder.

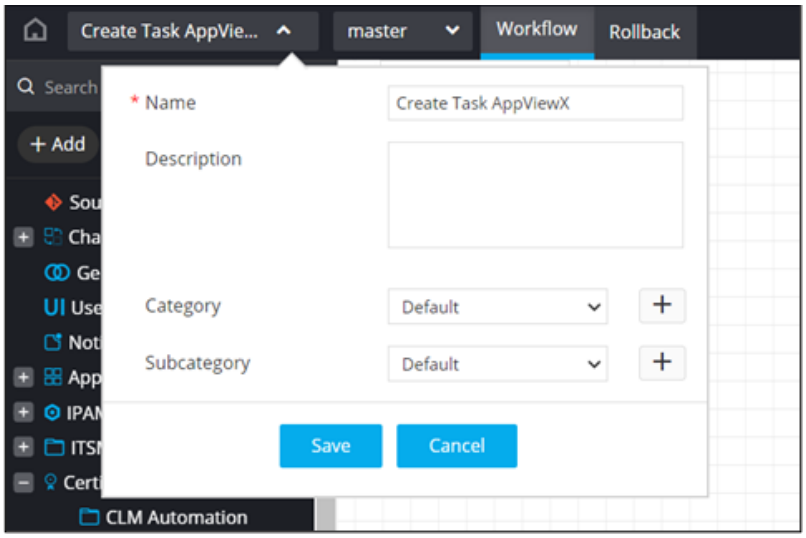
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



To design a custom workflow using **Enrollment** tasks:

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

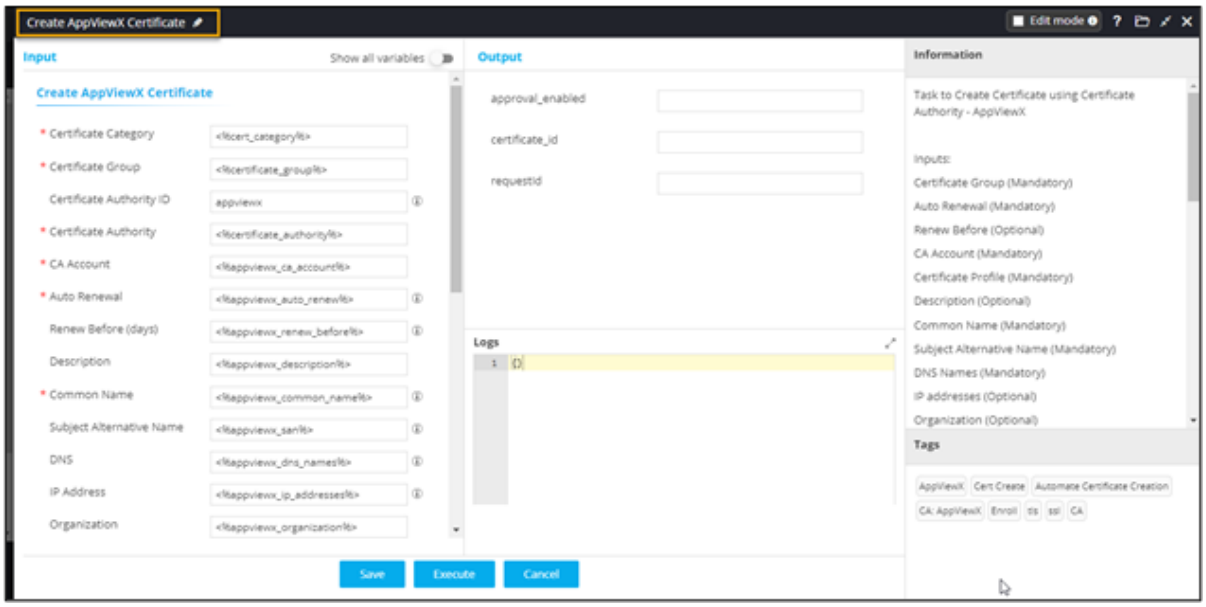


3. From the **Certificates** folder, click **Enrollment**.

   The tasks for the following CAs are available in the **Enrollment** folder:

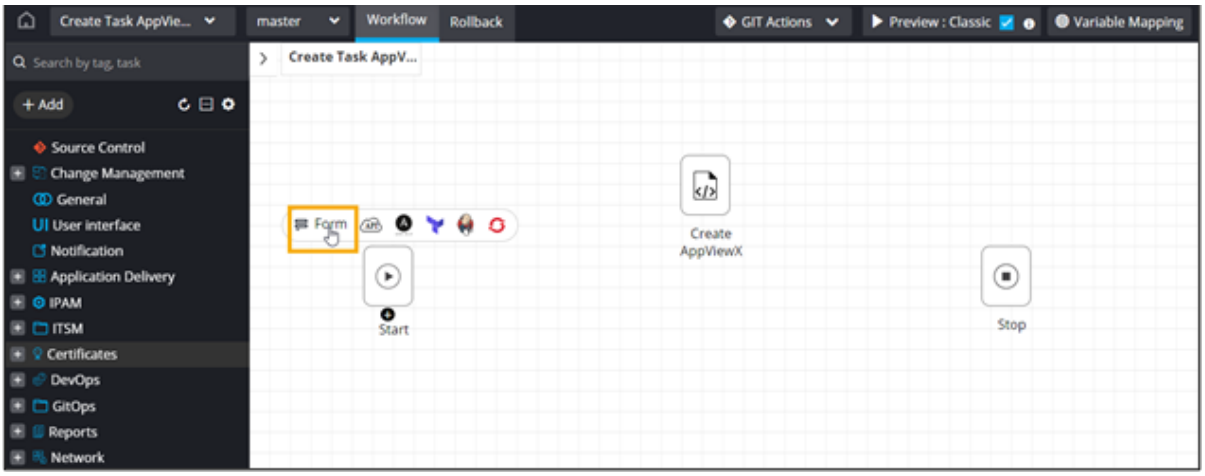
   - Appviewx
   - DigiCert
   - EJBCA
   - Entrust
   - Microsoft Enterprise
   - Microsoft Standalone
   - GoDaddy

4. From the **Enrollment** folder, drag and drop any of the Create Certificate tasks. For example, the **Create AppViewX Certificate** task.

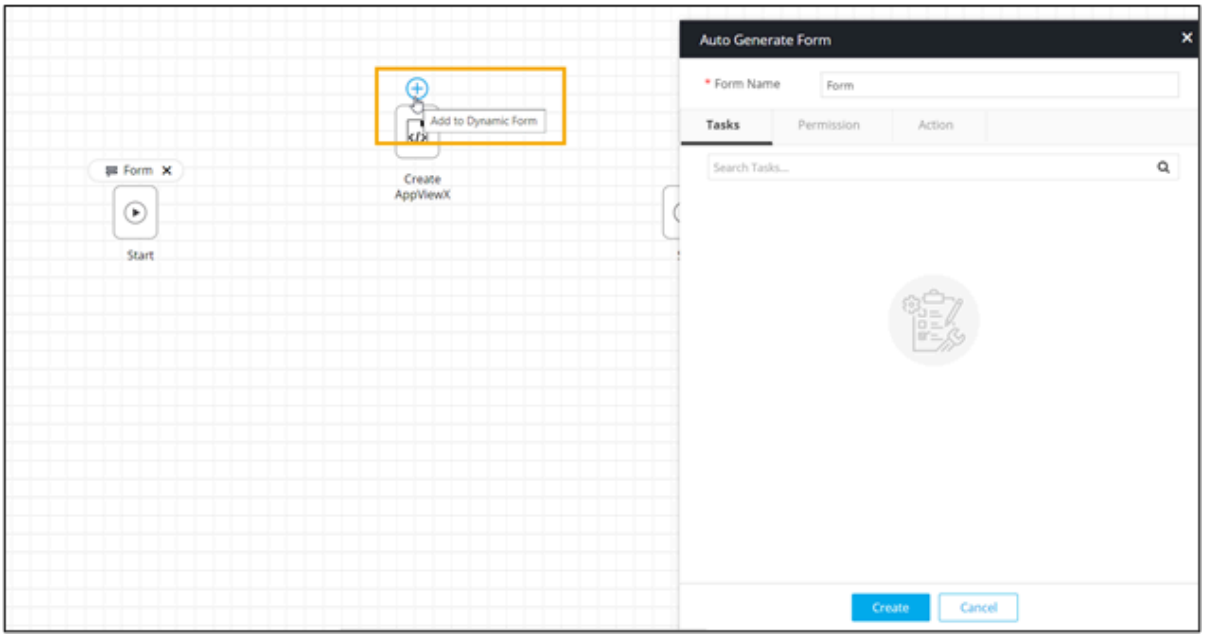


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **Save**.
6. To auto-generate a form for this workflow, click **Form** above the **Start** task.

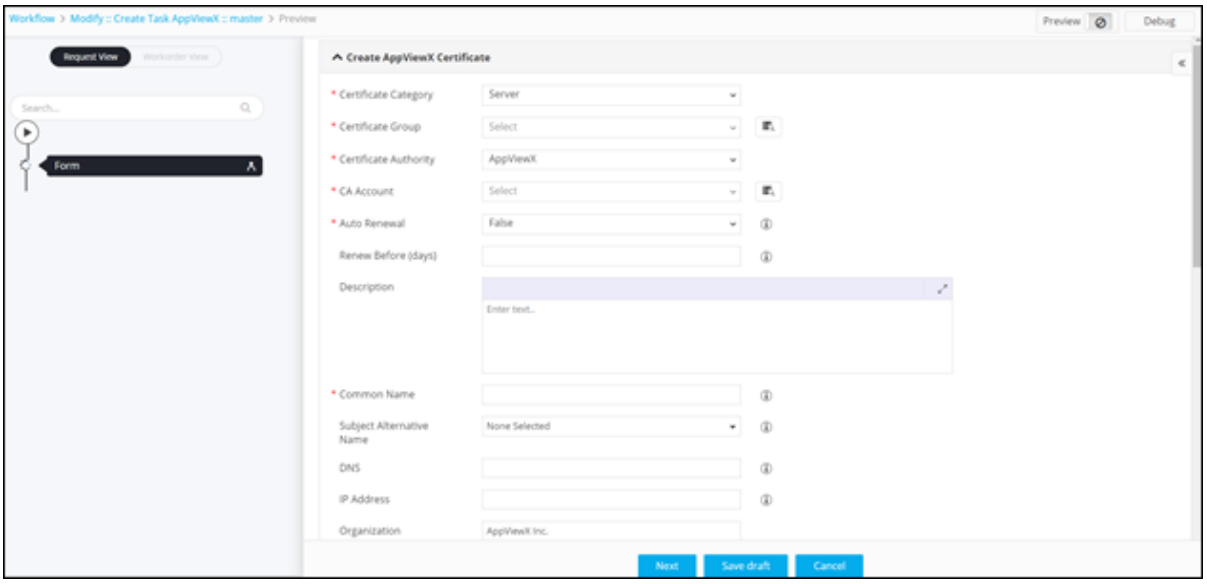


7. Click ⊕ above the **Create AppViewX** task to auto-populate the form fields.



8. Select the fields required in the input form.
9. Enter a **Form Name** and click **Create**.
10. To view and download the certificate in a holistic view, from the **Utils** folder, drag and drop the **View and Download Certificate** prebuilt task.
11. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.
    User Inputs form, when the **Create AppViewX Certificate** task is selected, is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field Description for the User Inputs form

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the **Certificate Group** field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the **CA Account** field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.
Renew Before (days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date.

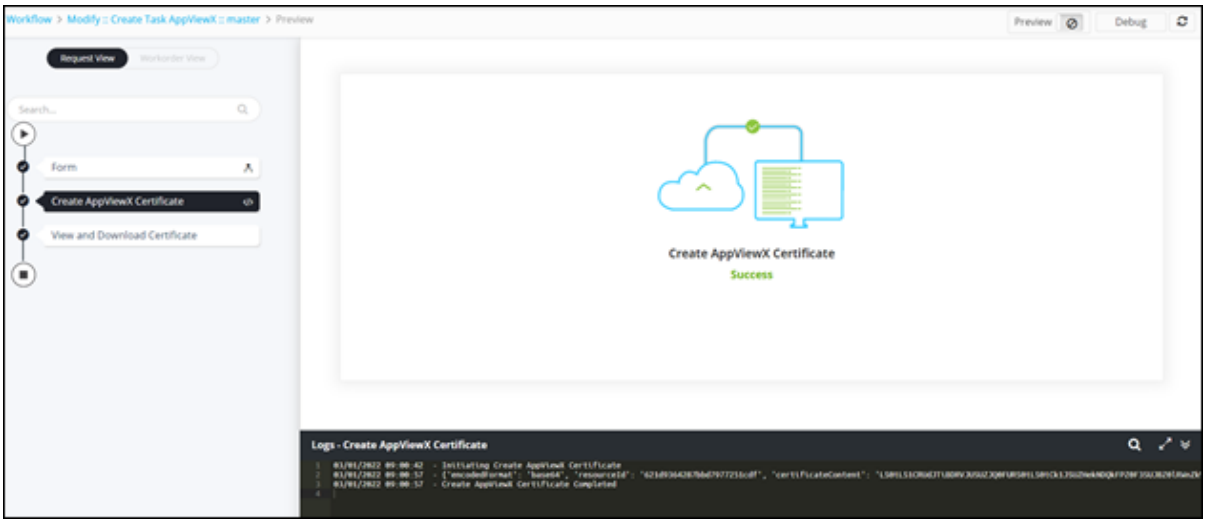
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Add a description for the workflow, if required.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the Zip code in which the organization is located.
Email Address	Enter the Email Address of the organization.
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the Validity Unit selected.
Challenge Password	Enter the challenge password.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

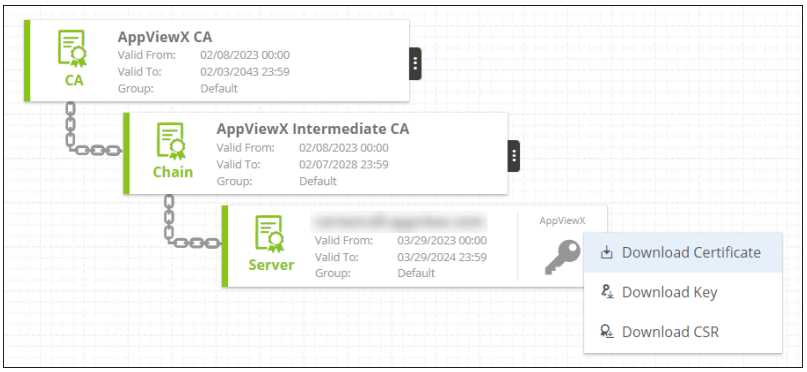
Field	Description
	Note: To retrieve the types of keys that can be availed, click .
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All asterisk (*) marked fields are mandatory.	

12. To add the attribute to the **Certificate Attributes** grid, click .
13. To edit the value of a particular attribute, select the attribute in the grid and click .
14. Enter the new value for the attribute in the **Value** field and click again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Click **Next**.
    AppViewX Certificate is created.

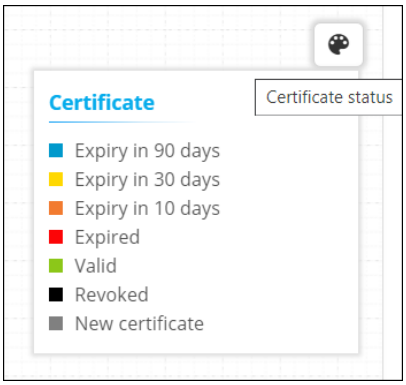


19. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



20. Hover your mouse over to view the **Certificate status**.



Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Renew Tasks

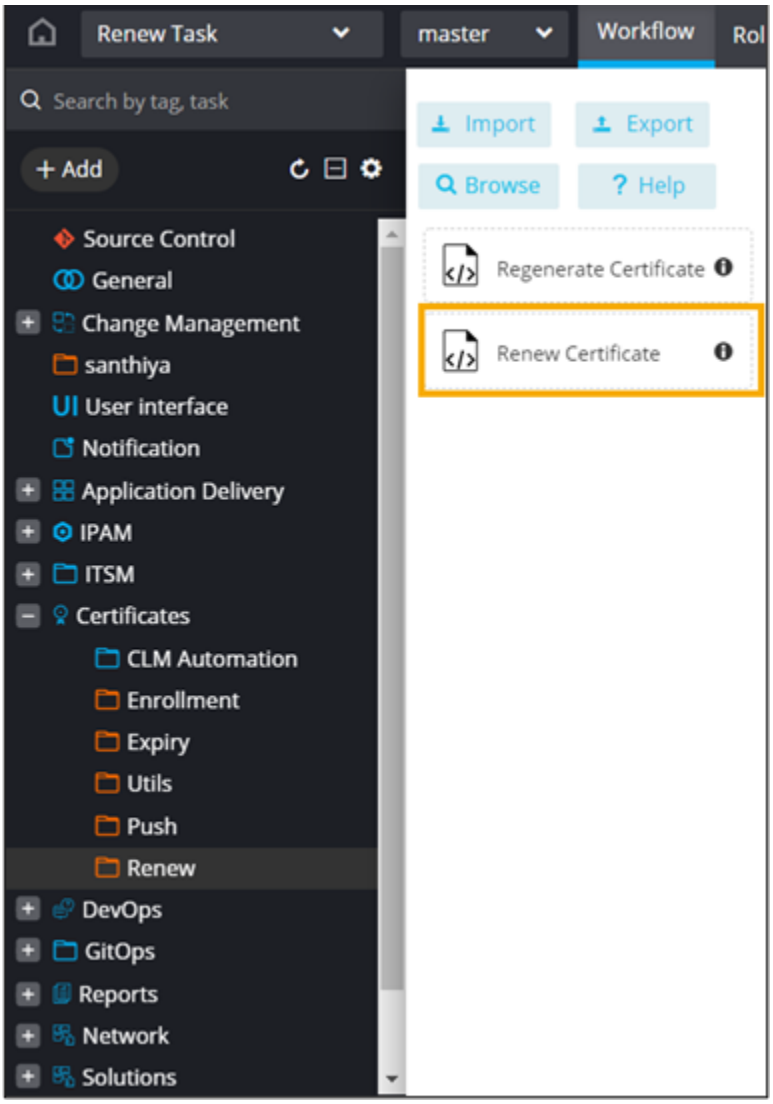
This section describes the **Renew** and **Regenerate** tasks that can be integrated with custom workflows to renew and regenerate certificates.

- Renew Task
- Regenerate Task

Renew Task

The OOB script task for renewing certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.

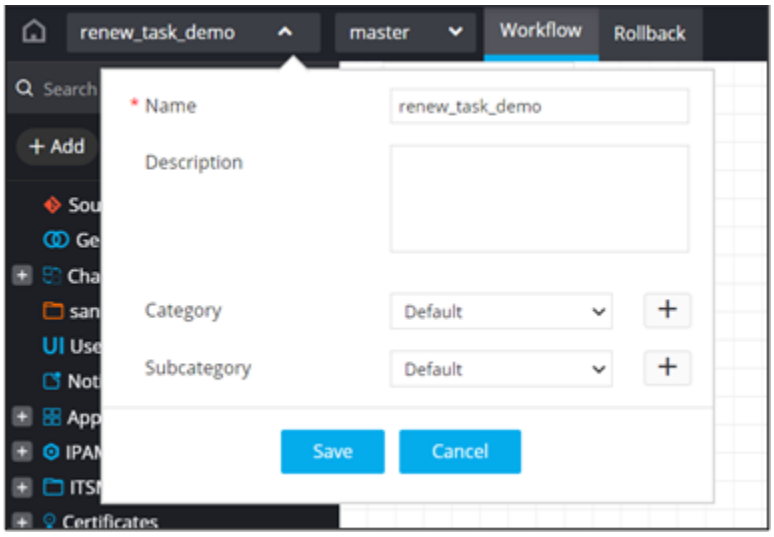
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



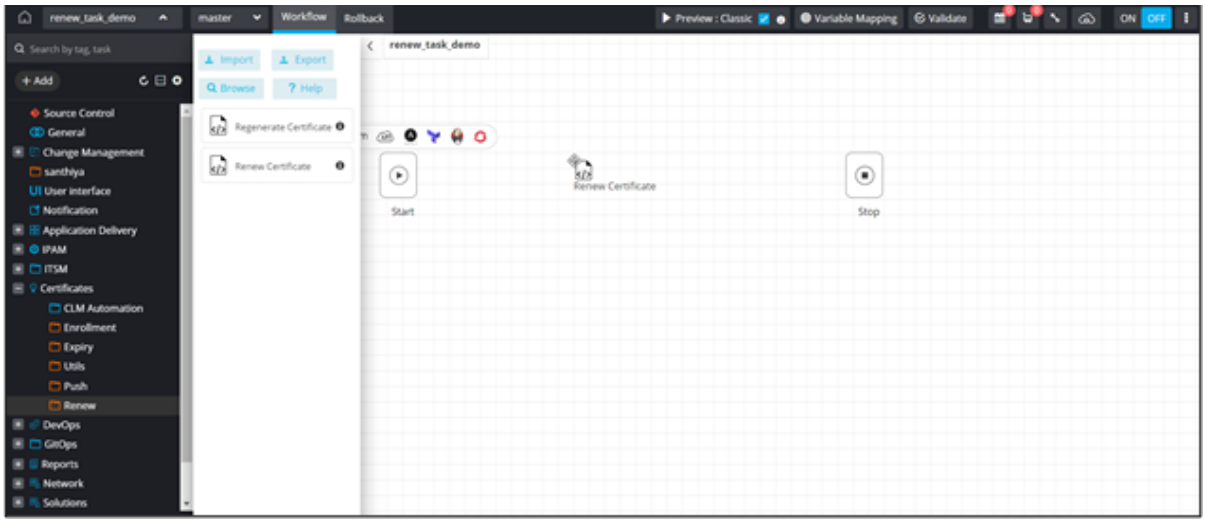
To design a custom workflow using the **Renew** task:

1. Navigate to the WorkflowWorkflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

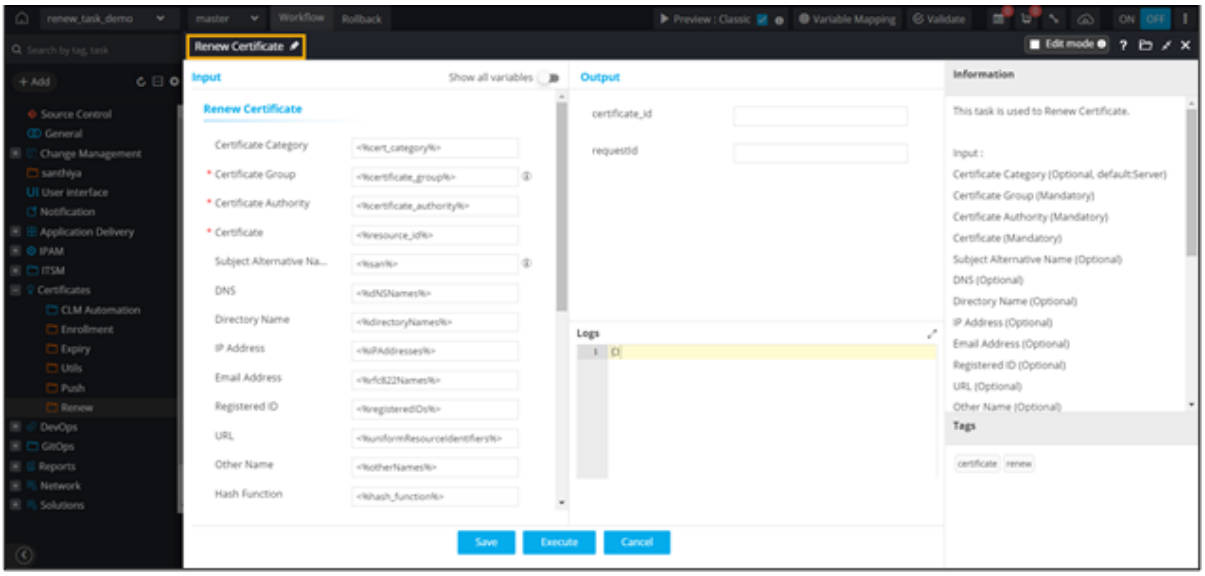


3. From the **Certificates** folder, under **Renew**, drag and drop the **Renew Certificate** task.

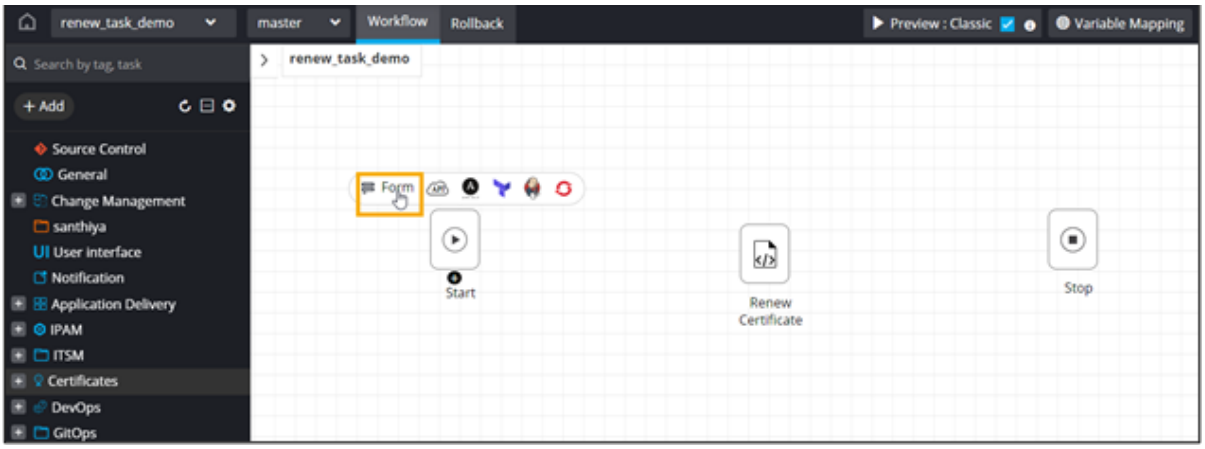


This task can be used to renew certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

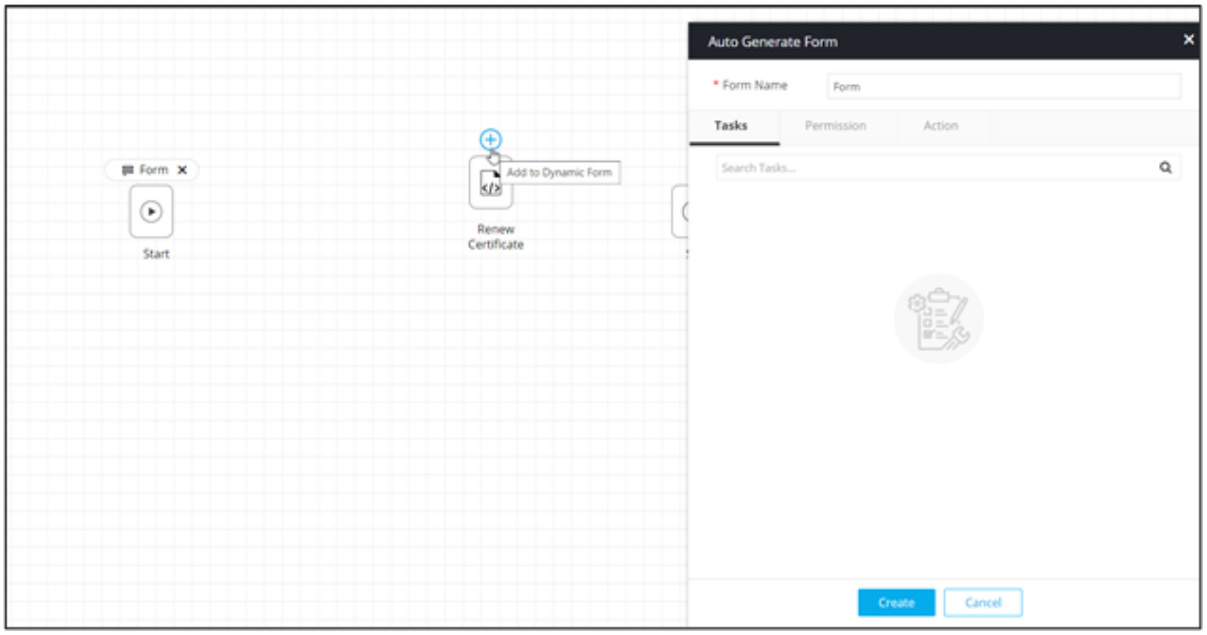


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.



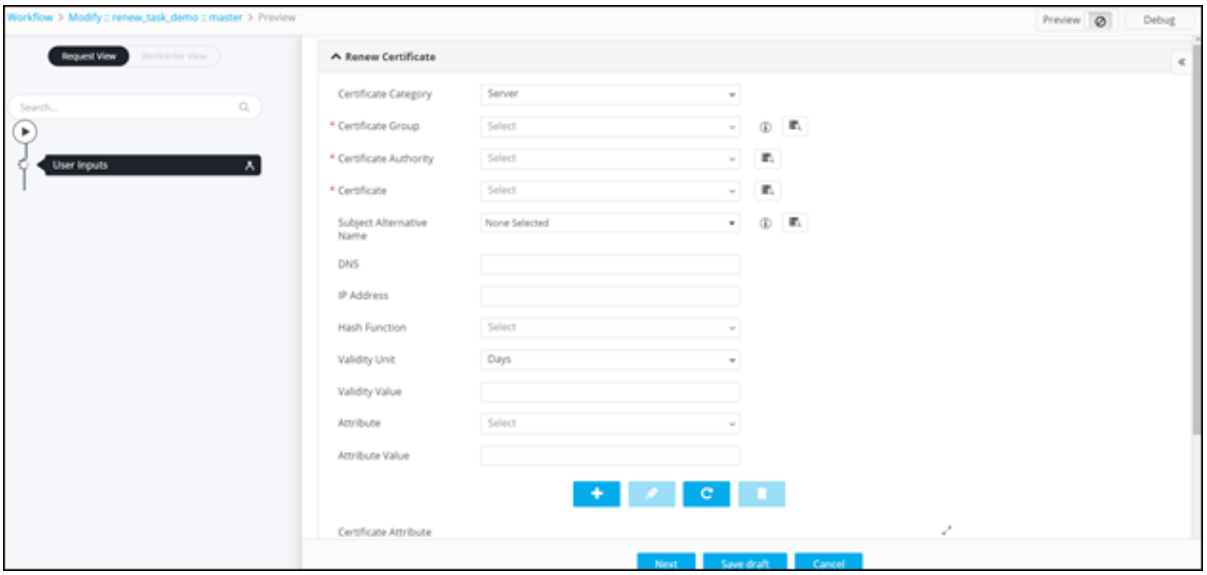
5. Click ⊕ above the **Renew Certificates** task to auto-populate the form fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Provide a **Form Name** and click **Create**.
8. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.
9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

   The **User Inputs** form is displayed on the screen.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for the User Inputs form

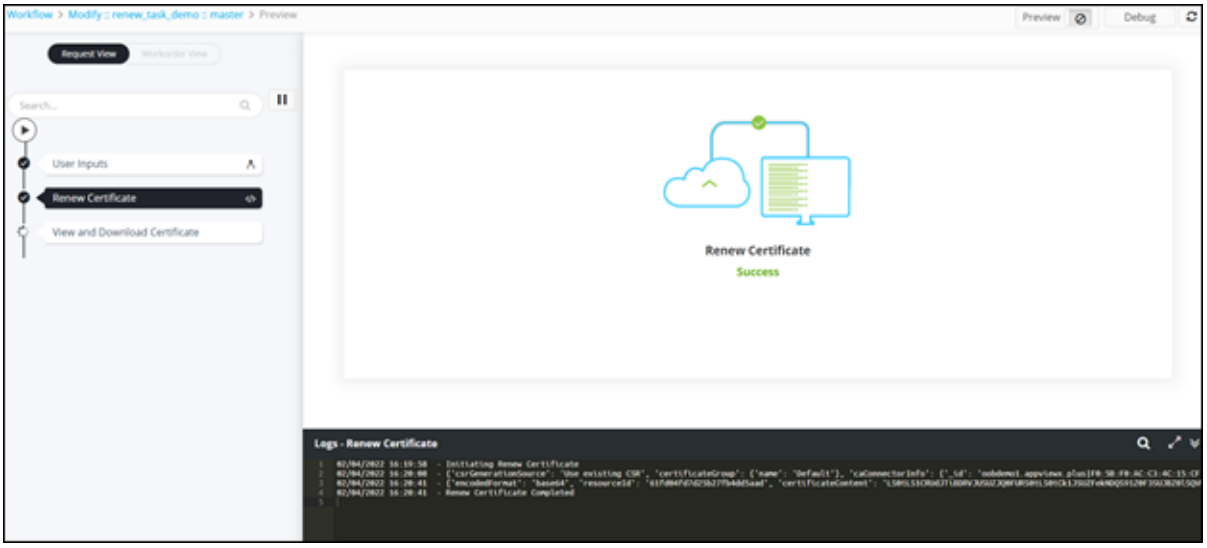
Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
Validity Unit	Select the **Validity Unit** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Validity Value	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

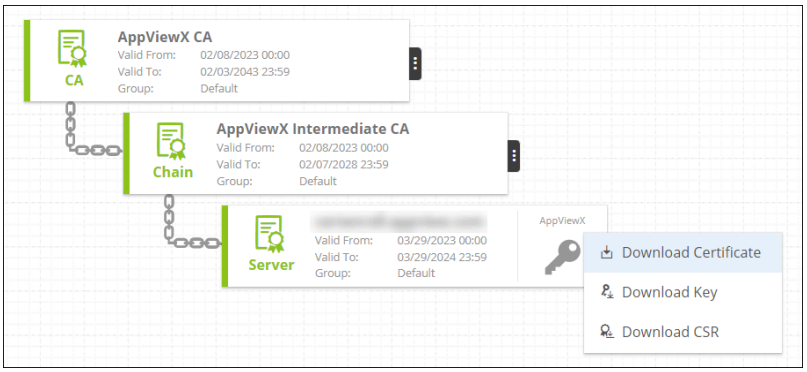
10. To add this attribute to the **Certificate Attributes** grid, click .
11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Click **Next**.

    Certificate renewed successfully.

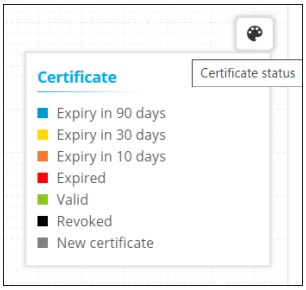


17. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



18. Hover your mouse over to view the **Certificate status**.



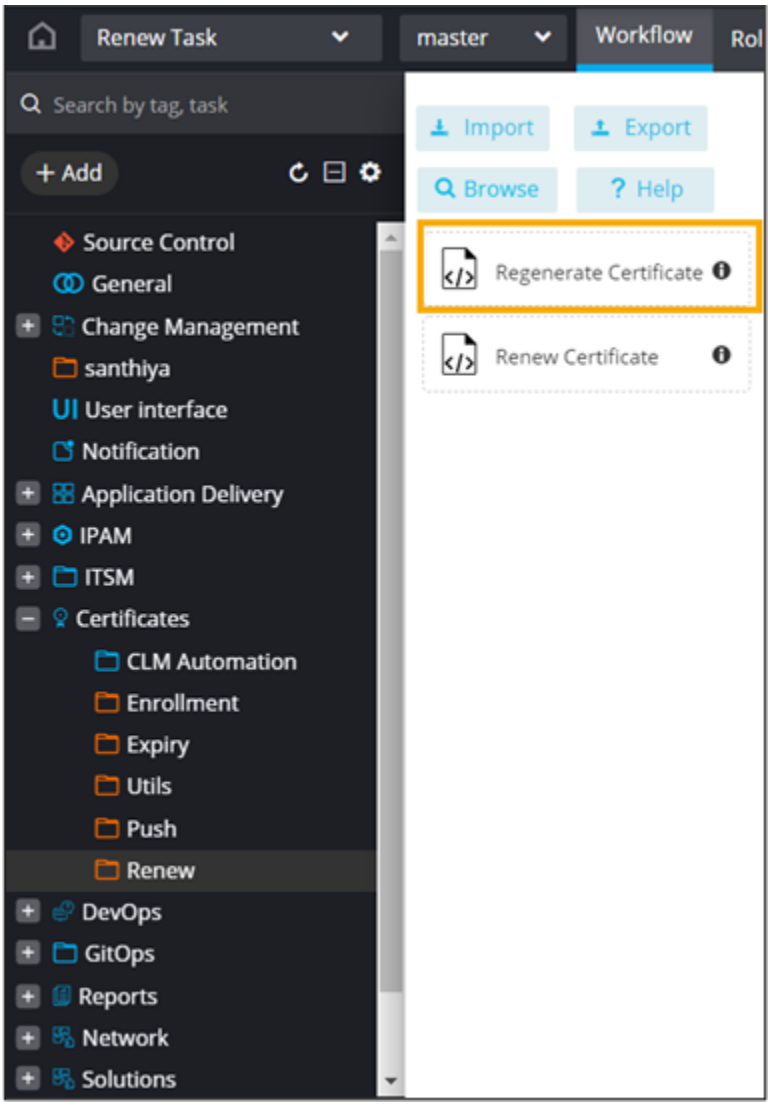
19. Click on the renewed certificate to view the **Certificate Details**.

> **Note:** For more information on how to design custom workflows, refer to the Automation User Guide.

Regenerate Task

The OOB script task for regenerating certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.

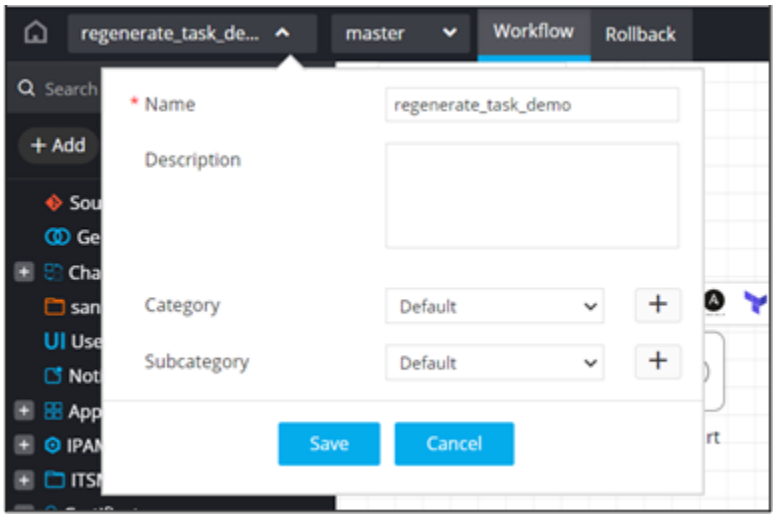
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



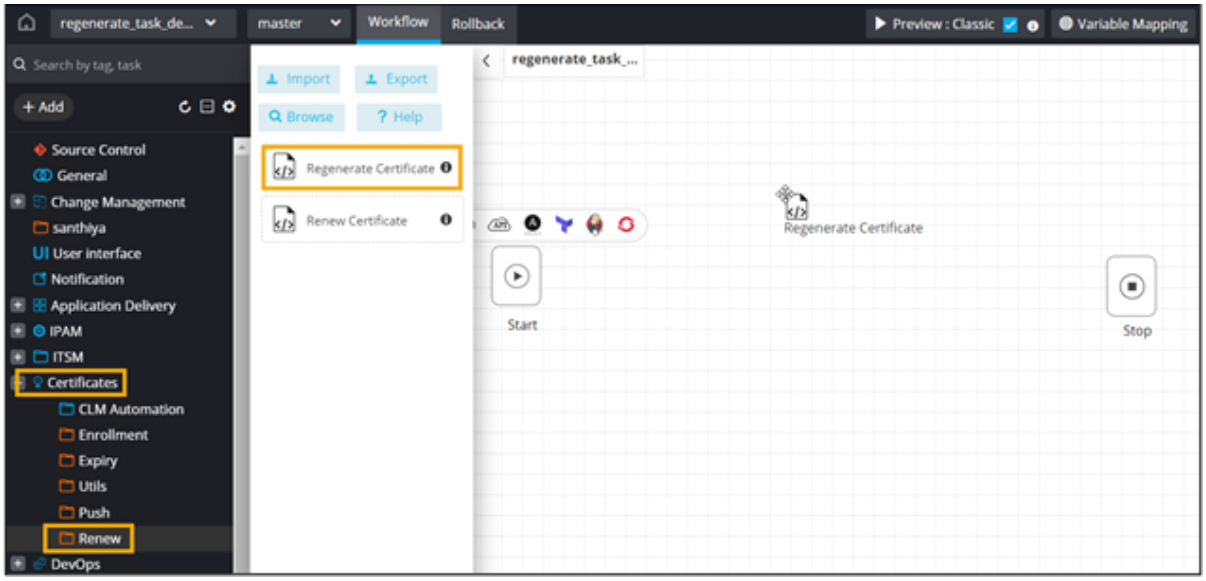
To design a custom workflow using the **Regenerate** task:

1. Navigate to the WorkflowWorkflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

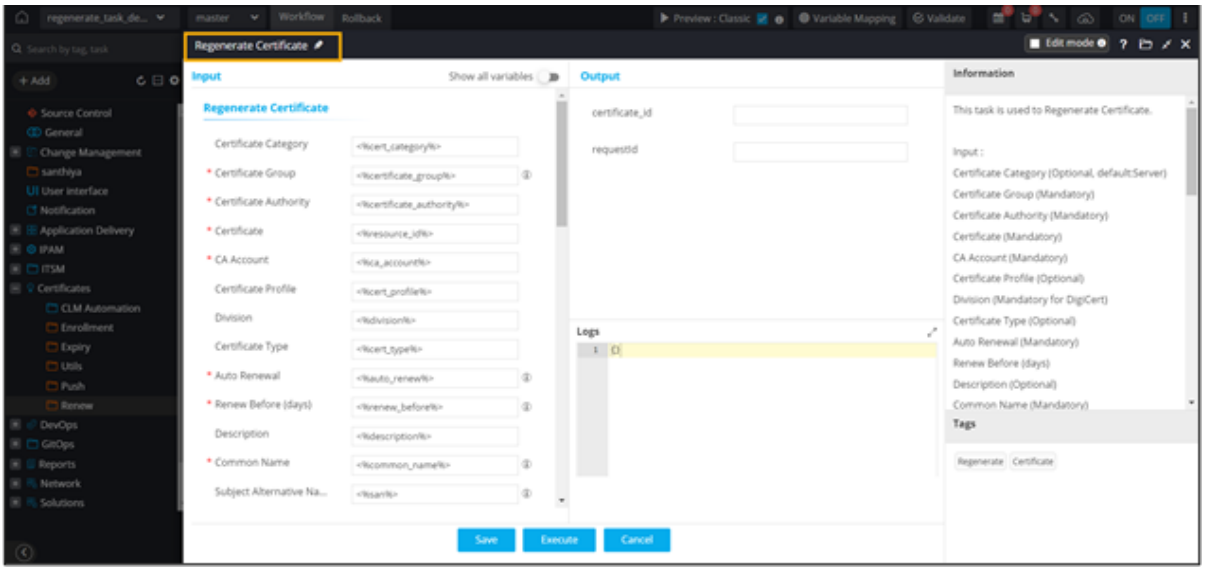


3. From the **Certificates** folder, under **Renew**, drag and drop the **Regenerate Certificate** task.

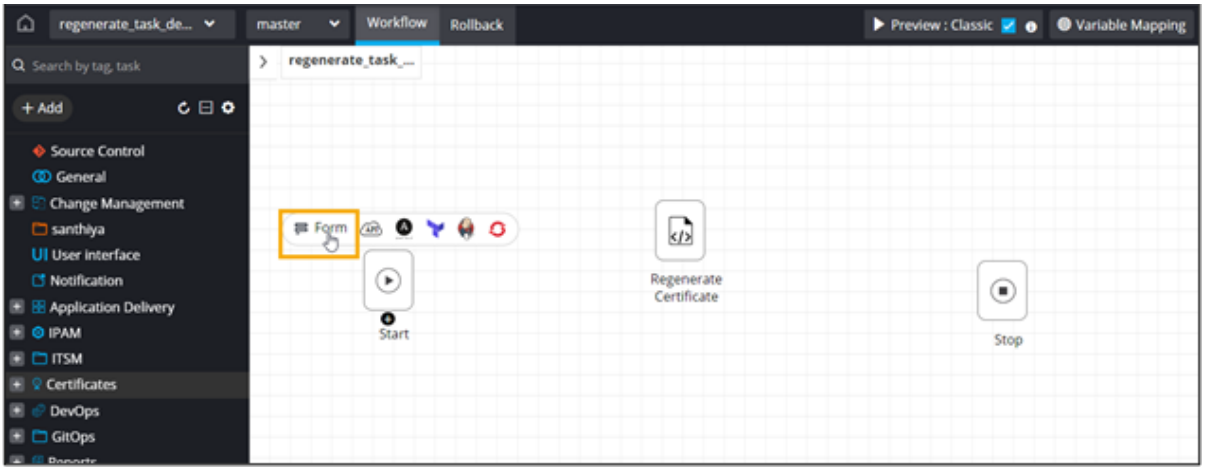


This task can be used to regenerate certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

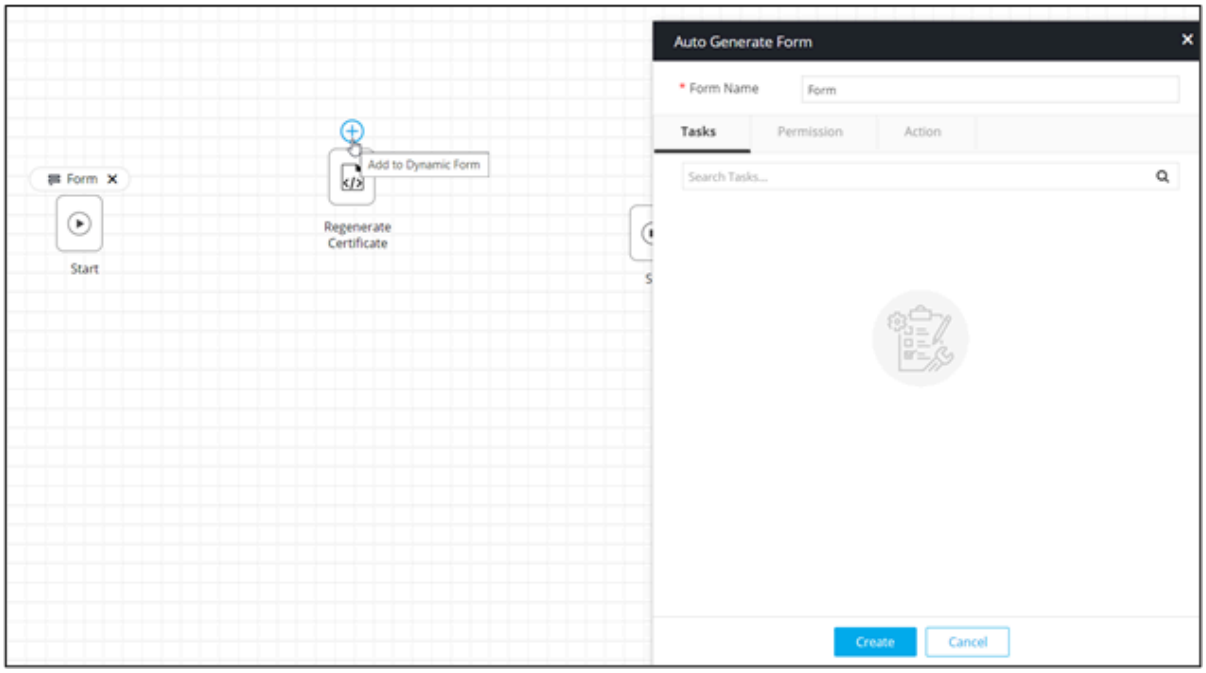


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.

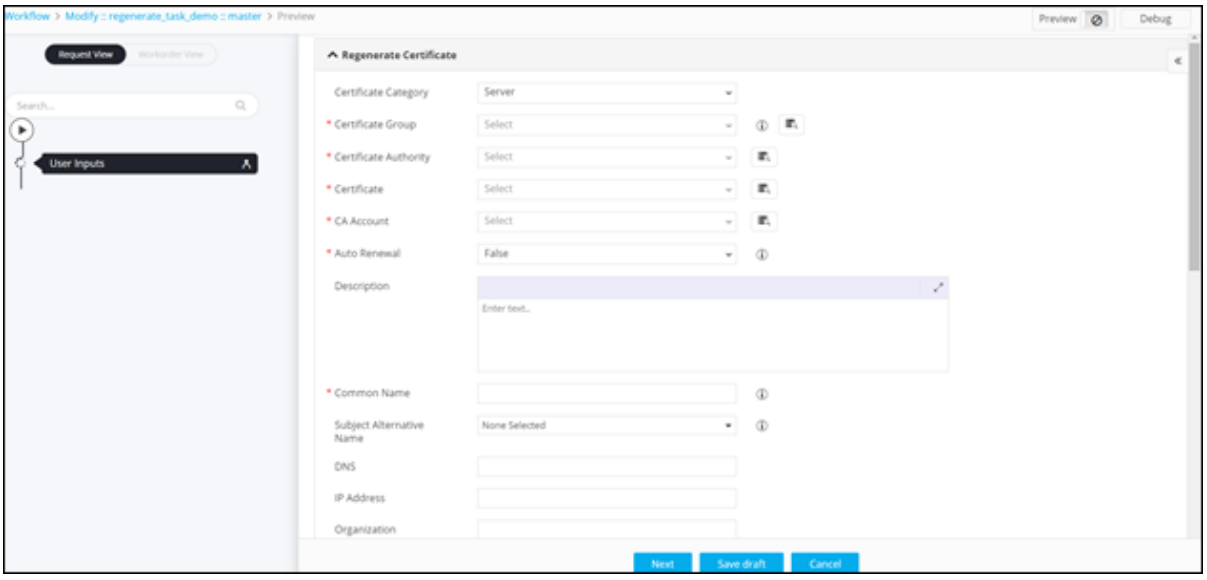


5. Click ⊕ above the **Regenerate Certificates** task to auto-populate the form fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Enter a **Form Name** and click **Create**.
8. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.
9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.
   The **User Inputs** form is displayed on the screen.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for the User Inputs form

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the CA Account field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.
Description	Provide a description for the regenerated certificate.
***Common Name**	This field is populated on the basis of the certificate selected.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
City	Enter the name of the city in which the organization is located.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the organization.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type**from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** To retrieve the values in the Bit Length field, click .
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

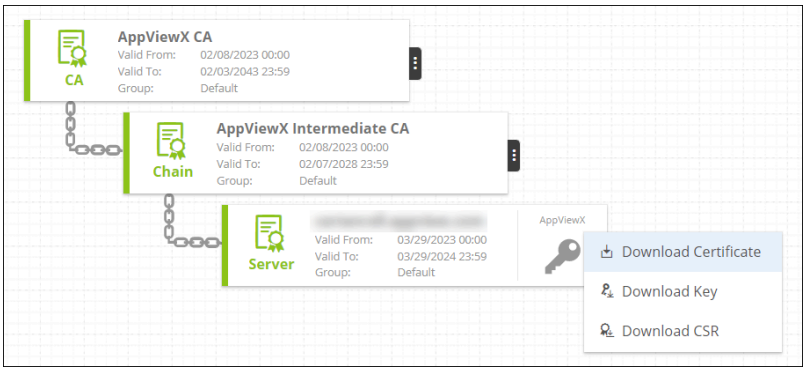
10. To add this attribute to the **Certificate Attributes** grid, click .
11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

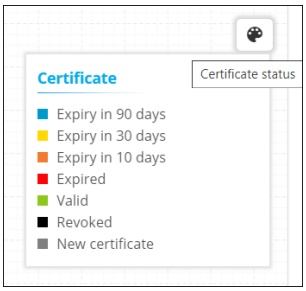
16. Click **Next**.

    Certificate is regenerated successfully.

17. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over ⋮ and from the options displayed, click **Download Certificate**.



18. Hover your mouse over 🎨 to view the **Certificate status**.



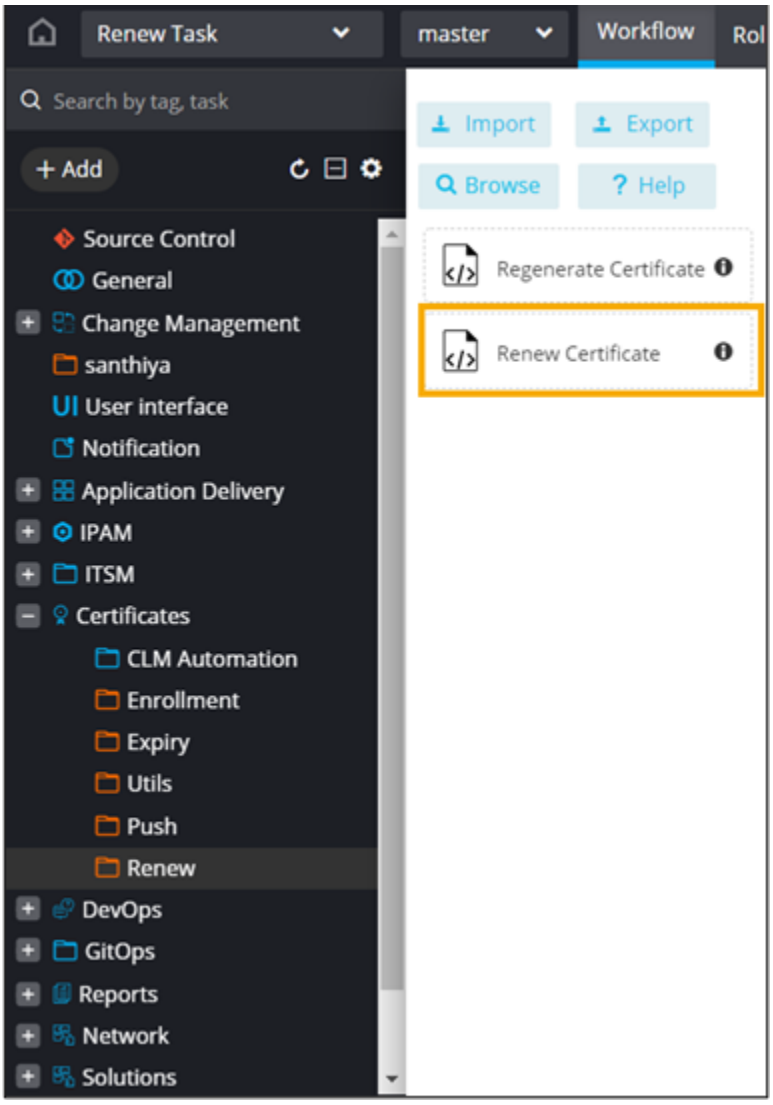
19. Click on the regenerated certificate to view the **Certificate Details**.

Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Renew Task

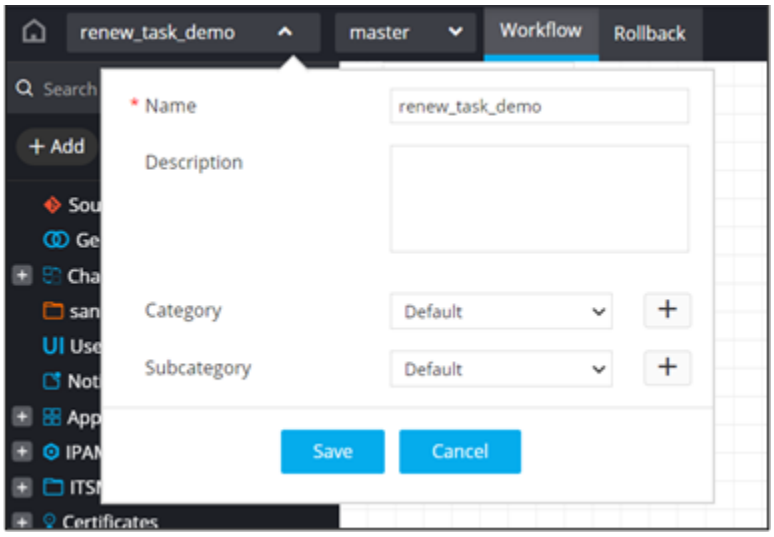
The OOB script task for renewing certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.



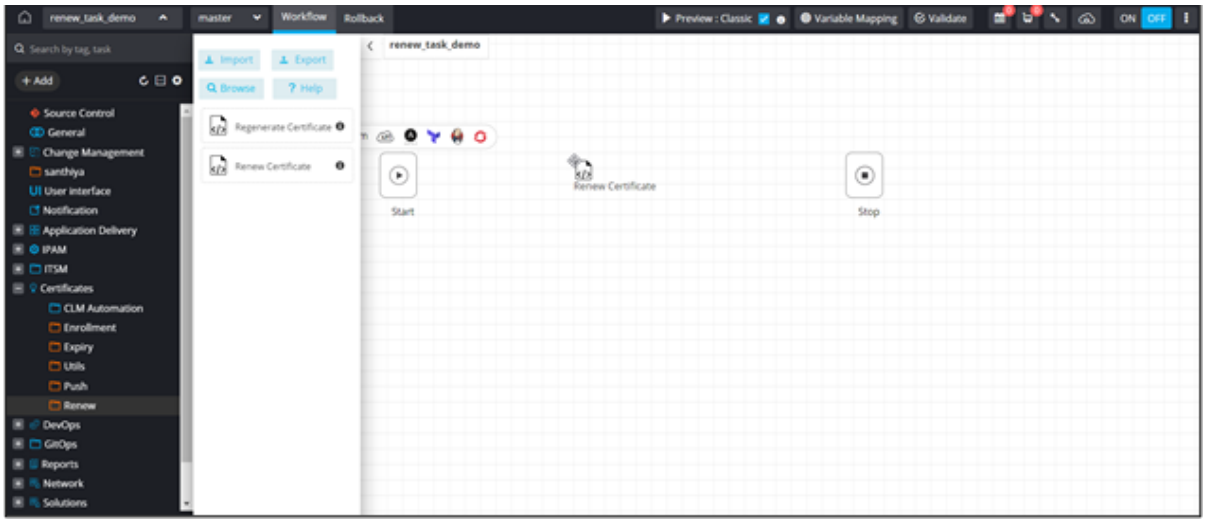
To design a custom workflow using the **Renew** task:

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

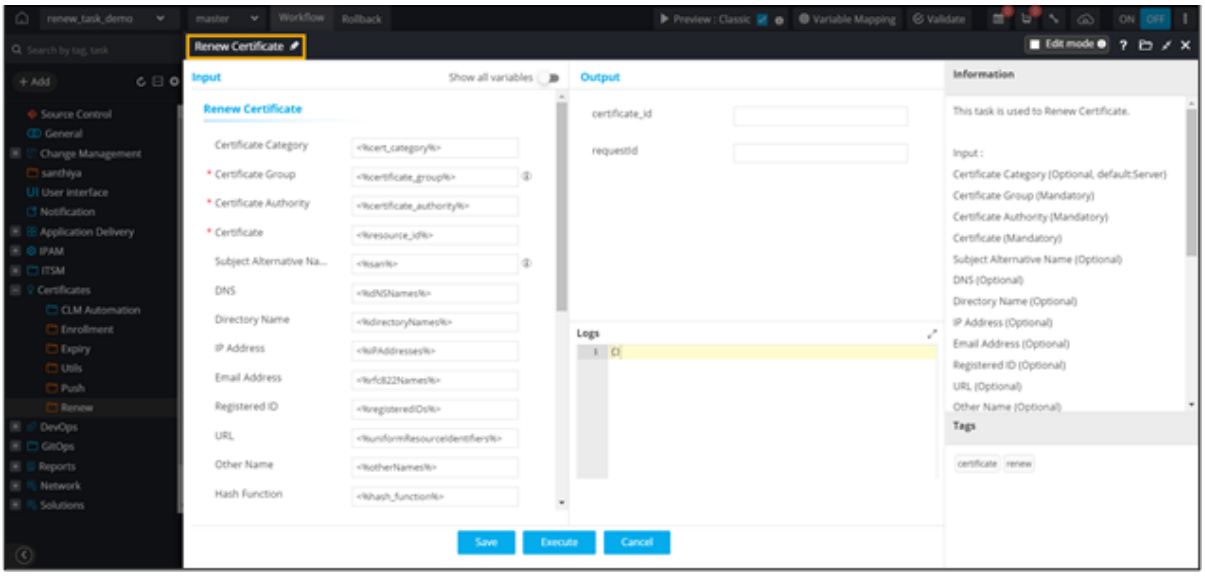


3. From the **Certificates** folder, under **Renew**, drag and drop the **Renew Certificate** task.

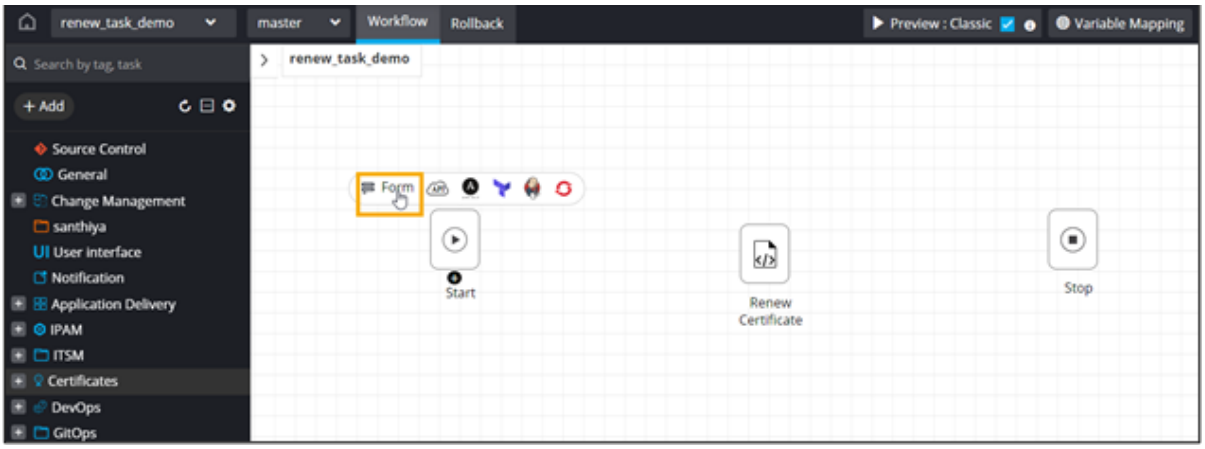


This task can be used to renew certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

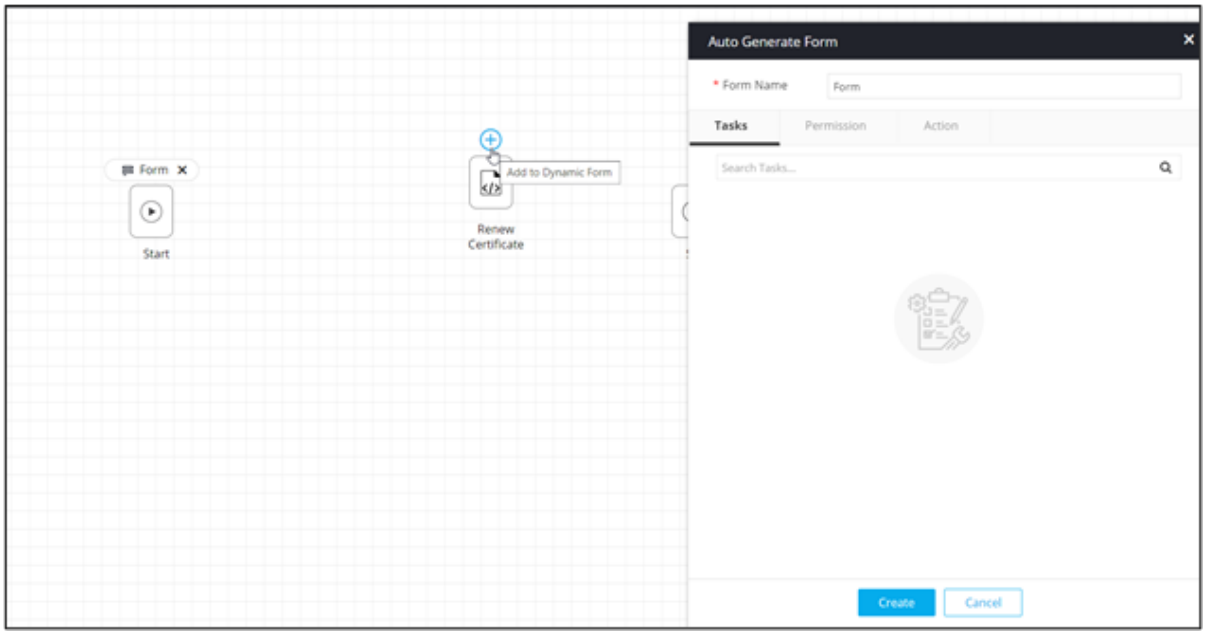


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.



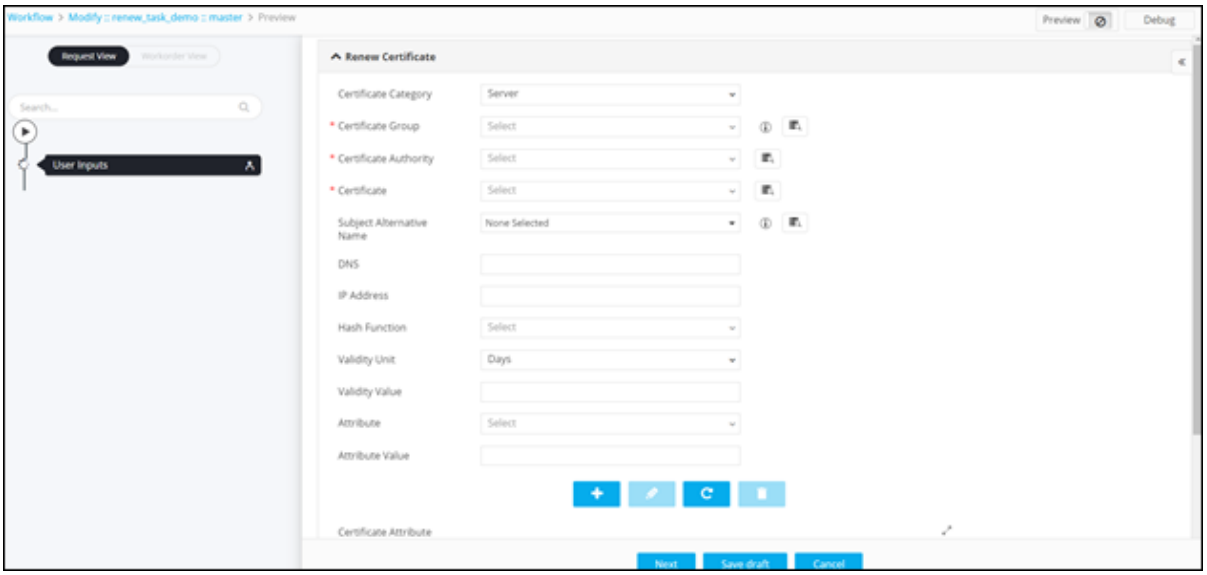
5. Click ⊕ above the **Renew Certificates** task to auto-populate the form fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Provide a **Form Name** and click **Create**.
8. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.
9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

   The **User Inputs** form is displayed on the screen.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for the User Inputs form

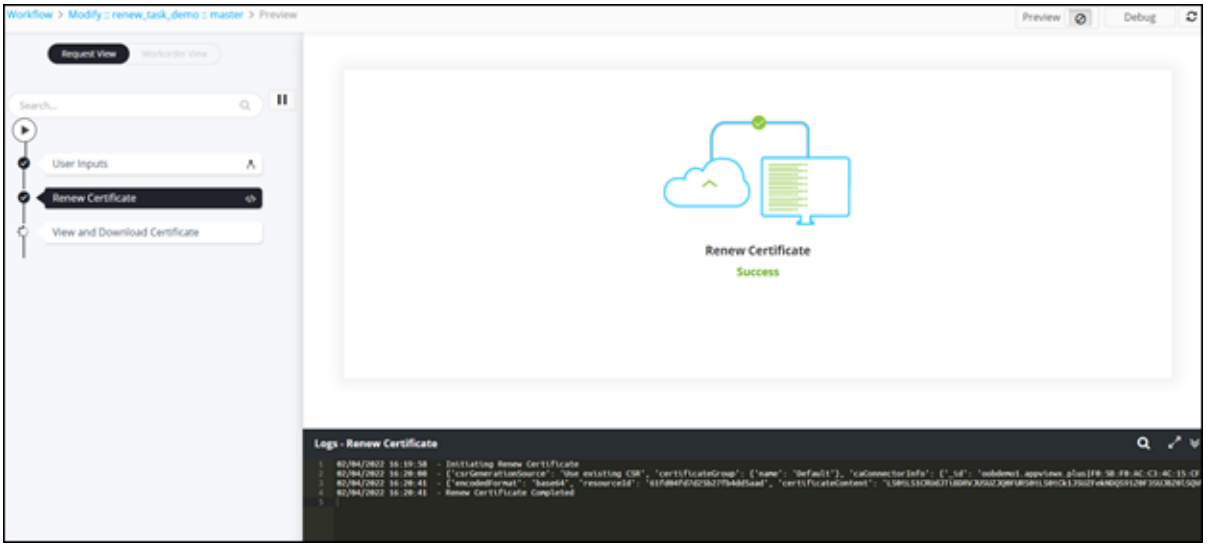
Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown. **Note:** To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Hash Function	Select the **Hash Function** from the options available in the dropdown.
Validity Unit	Select the **Validity Unit** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Validity Value	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

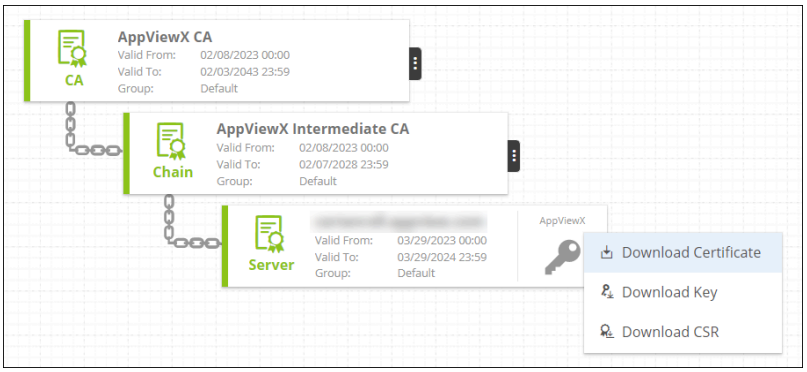
10. To add this attribute to the **Certificate Attributes** grid, click .
11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Click **Next**.

    Certificate renewed successfully.

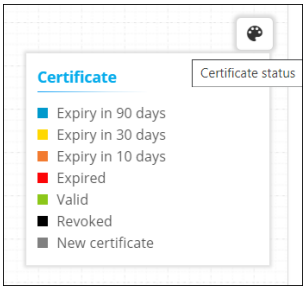


17. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



18. Hover your mouse over to view the **Certificate status**.



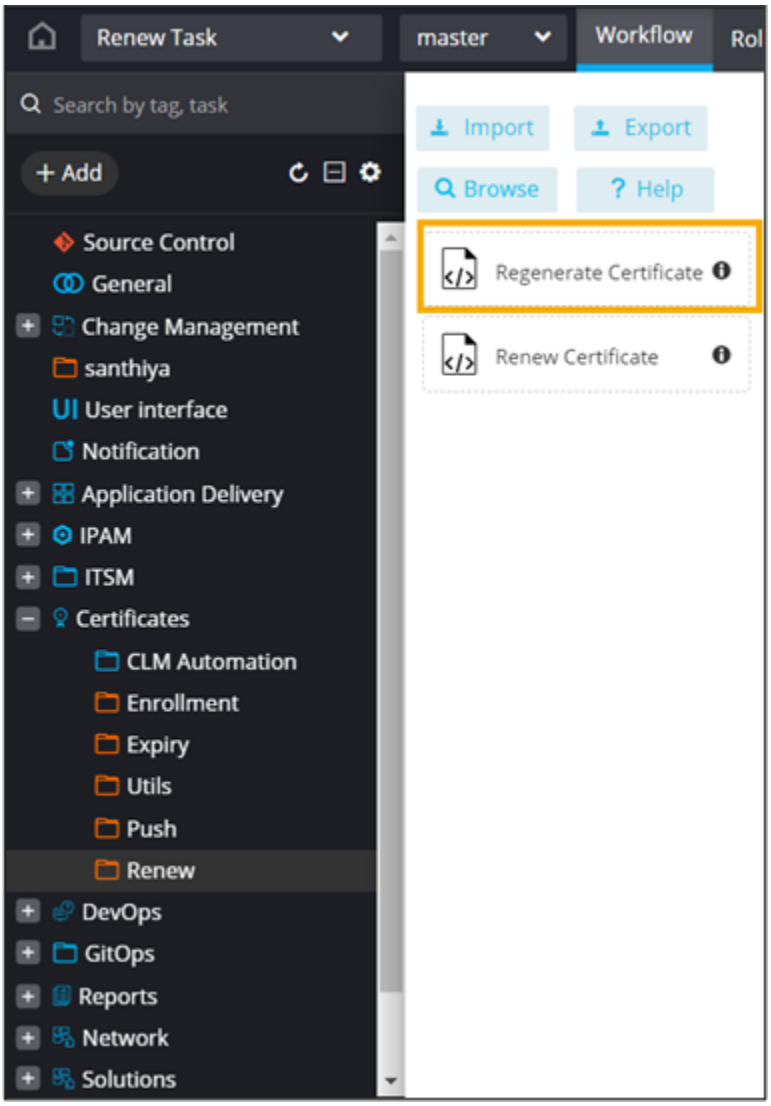
19. Click on the renewed certificate to view the **Certificate Details**.

Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Regenerate Task

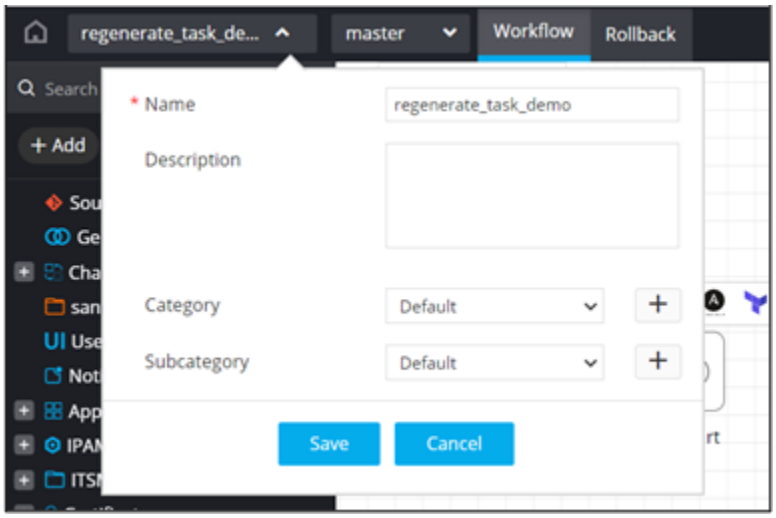
The OOB script task for regenerating certificates can be found in the **Workflow Studio**, under **Certificates**, in the **Renew** folder.



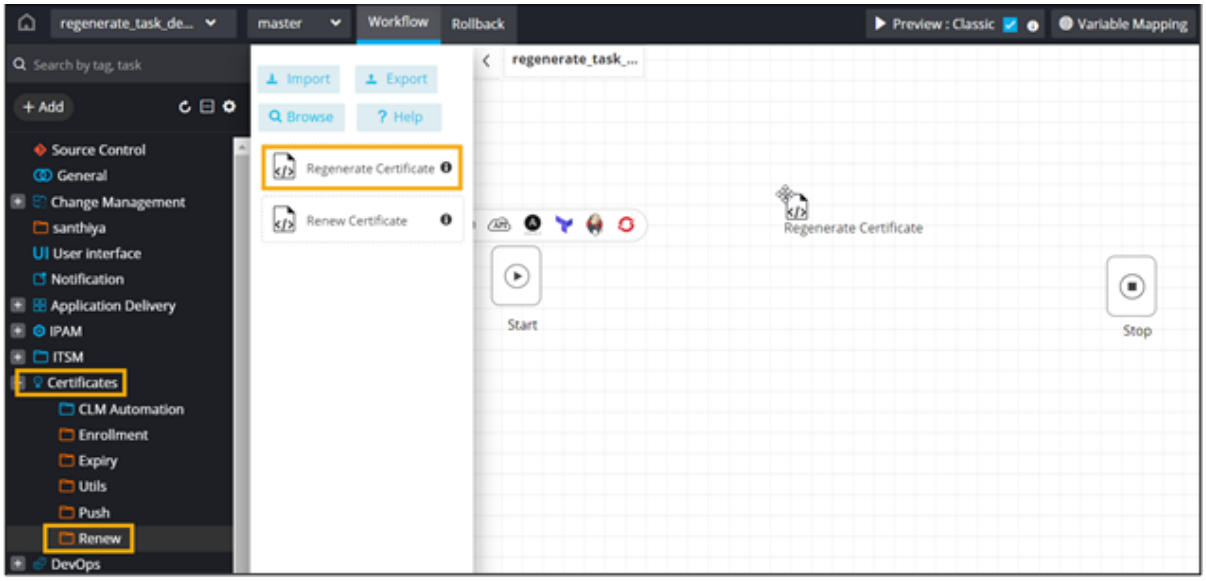
To design a custom workflow using the **Regenerate** task:

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

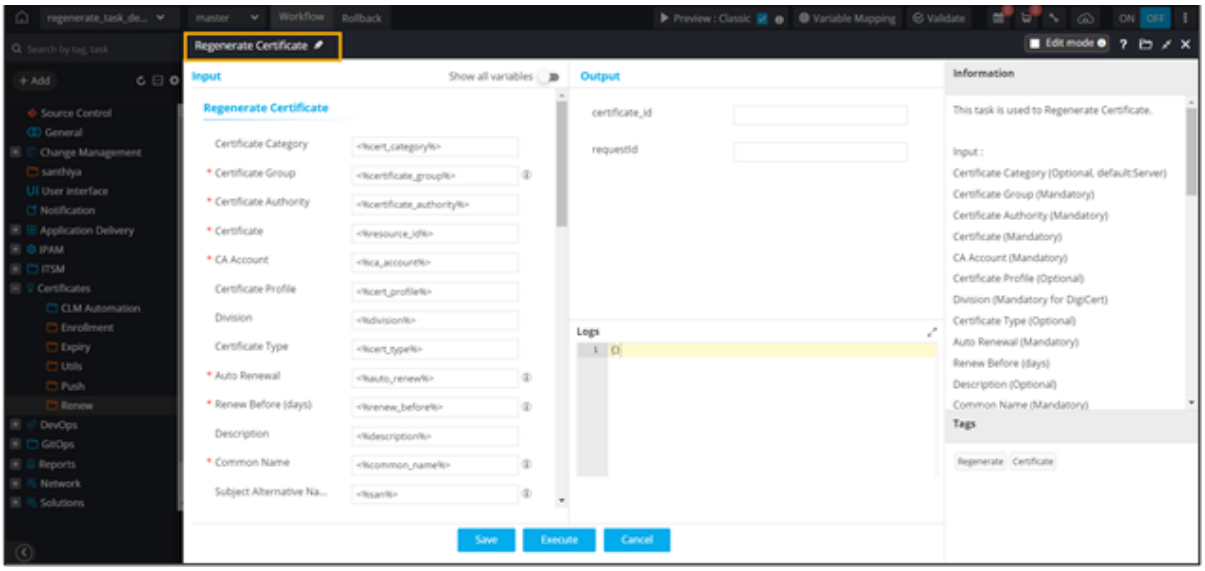


3. From the **Certificates** folder, under **Renew**, drag and drop the **Regenerate Certificate** task.

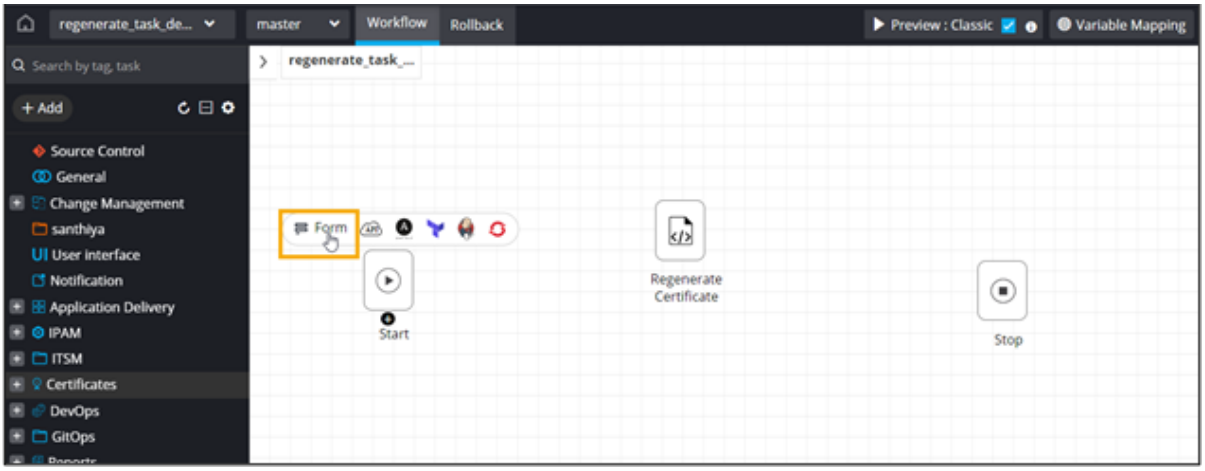


This task can be used to regenerate certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

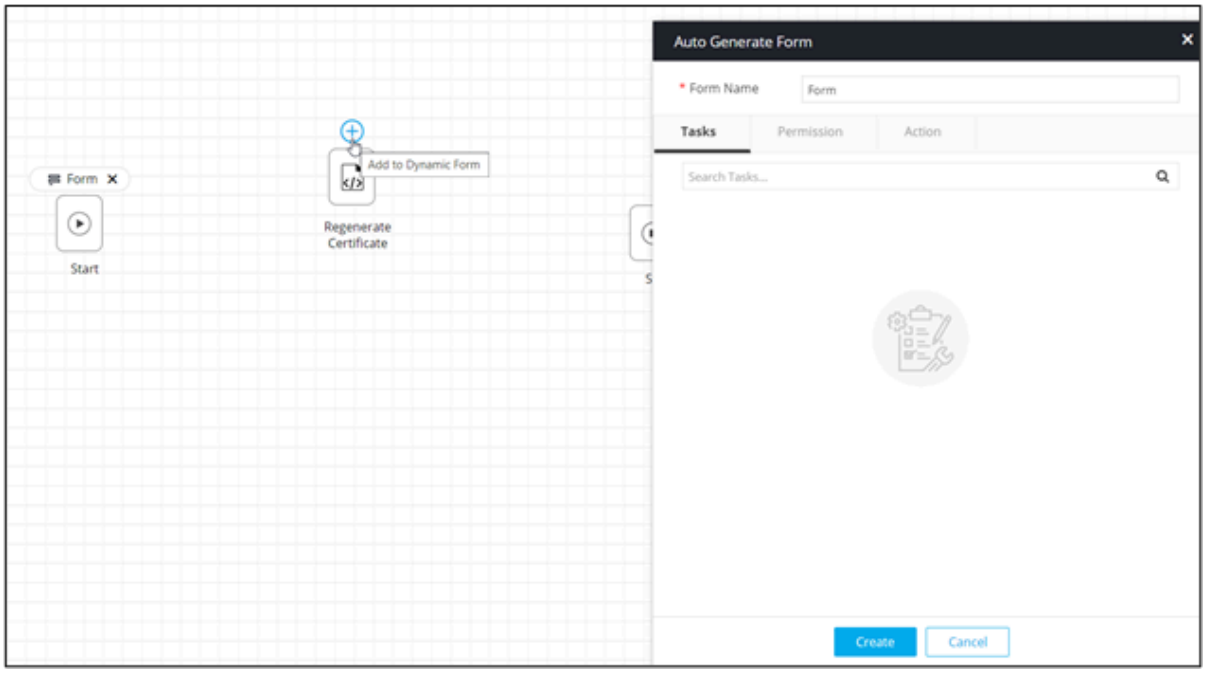


4. To auto-generate a form for this workflow, click **Form** above the **Start** task.

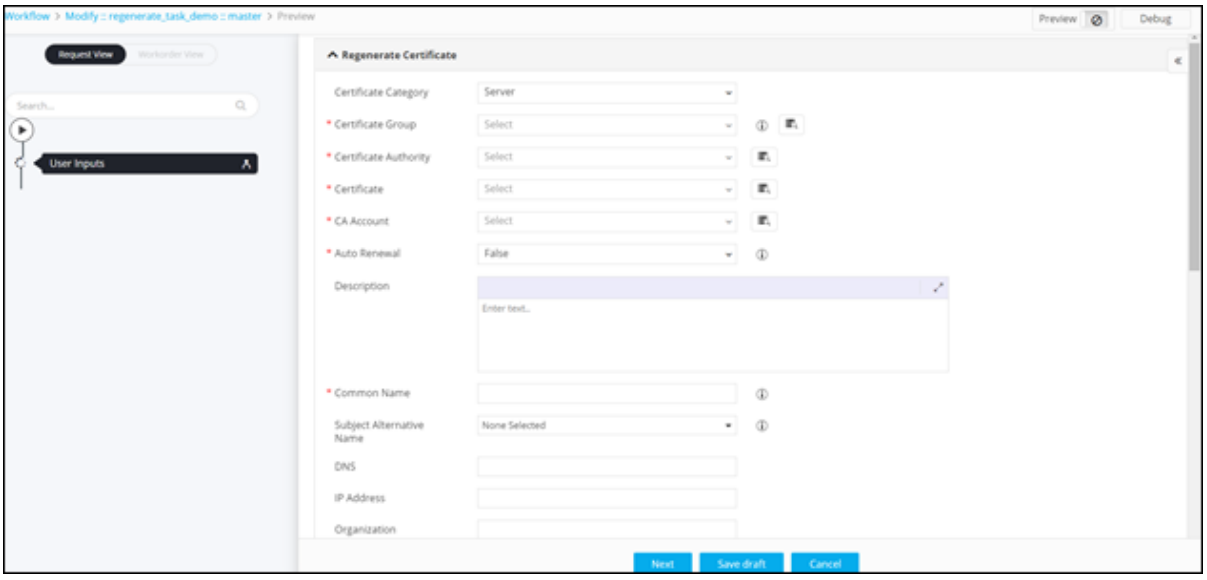


5. Click ⊕ above the **Regenerate Certificates** task to auto-populate the form fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Select the fields required in the input form.
7. Enter a **Form Name** and click **Create**.
8. From the **Utils** folder under the **Certificate** section, drag and drop the **View and Download Certificate** task.
9. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.
   The **User Inputs** form is displayed on the screen.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for the User Inputs form

Field	Description
Certificate Category	Select the **Certificate Category** from the options available in the dropdown. **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Group field, click .
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate Authority field, click .
***Certificate**	Select the **Certificate** from the options available in the dropdown. **Note:** To retrieve the values in the Certificate field, click .
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** To retrieve the values in the CA Account field, click .
***Auto Renewal**	Select the required option from the dropdown to enable/disable **Auto Renewal** for the regenerated certificate.
Description	Provide a description for the regenerated certificate.
***Common Name**	This field is populated on the basis of the certificate selected.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.

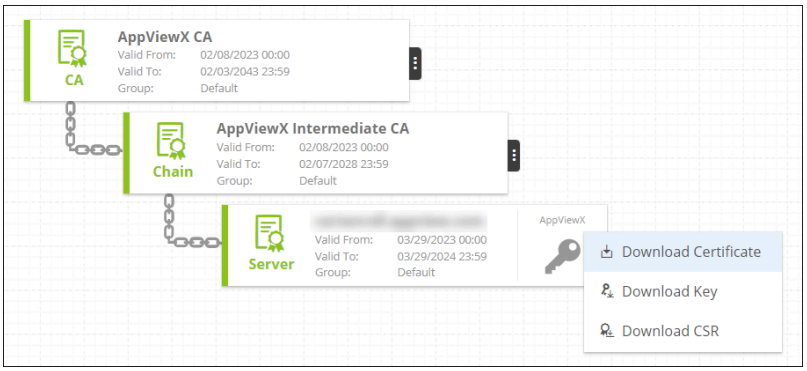
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: To retrieve the values in the Subject Alternative Name field, click .
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
City	Enter the name of the city in which the organization is located.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Email Address	Enter the email address associated with the organization.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type**from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** To retrieve the values in the Bit Length field, click .
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the **Validity Unit** selected.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.
All Asterisk (*) marked fields are mandatory.	

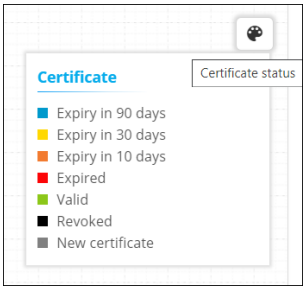
10. To add this attribute to the **Certificate Attributes** grid, click .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

11. To edit the value of a particular attribute, select the attribute in the grid and click .
12. Enter the new value for the attribute in the **Value** field and click again to update the value.
13. To delete a certificate attribute, select the attribute in the grid and click .
14. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
15. To search for a particular attribute in the grid, type the keyword(s) in the search field.
16. Click **Next**.
    Certificate is regenerated successfully.
17. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



18. Hover your mouse over to view the **Certificate status**.



19. Click the regenerated certificate to view the **Certificate Details**.

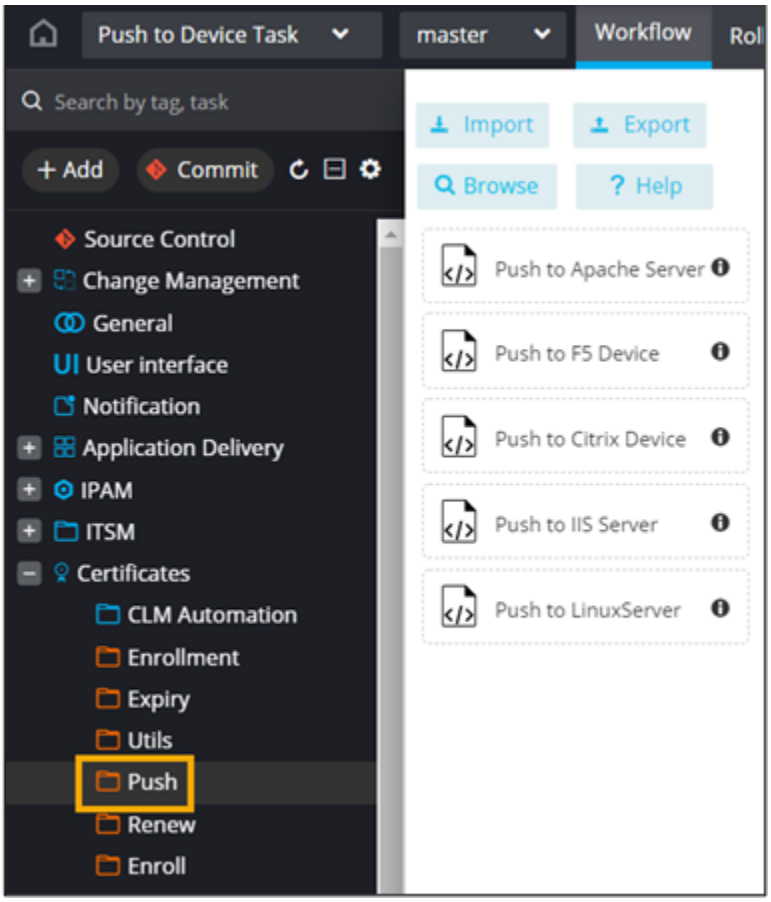
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: For more information on how to design custom workflows, refer to the Automation User Guide.

Push Tasks

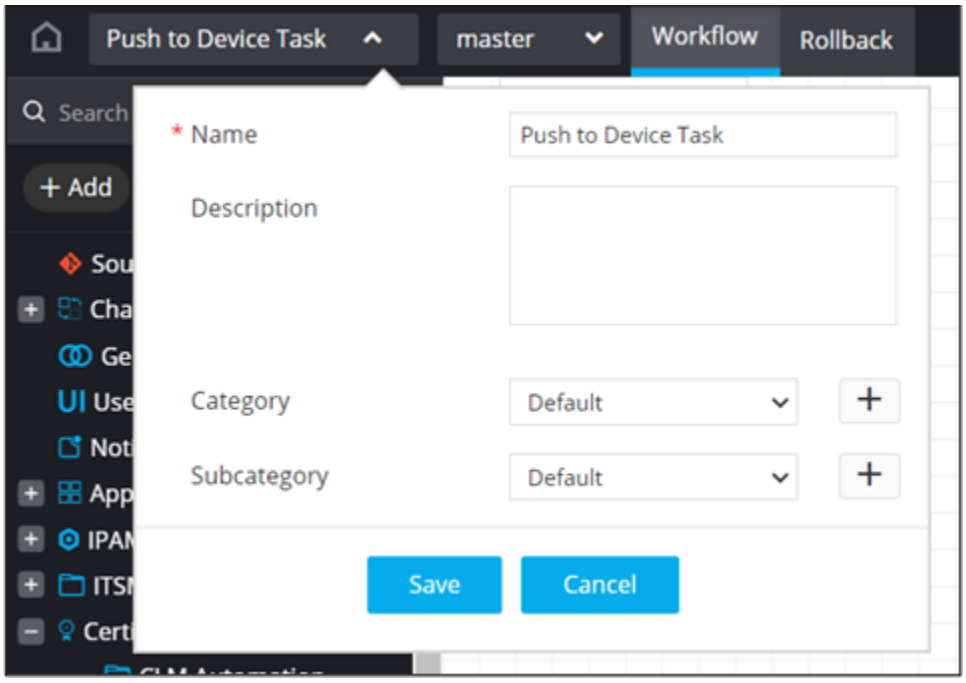
You can design a custom workflow for pushing a certificate to a device(s) or a server(s) using the prebuilt Push tasks available in the **Workflow Studio**. The OOB script task for pushing certificates to devices/ servers can be found under **Certificates**, in the **Push** folder.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



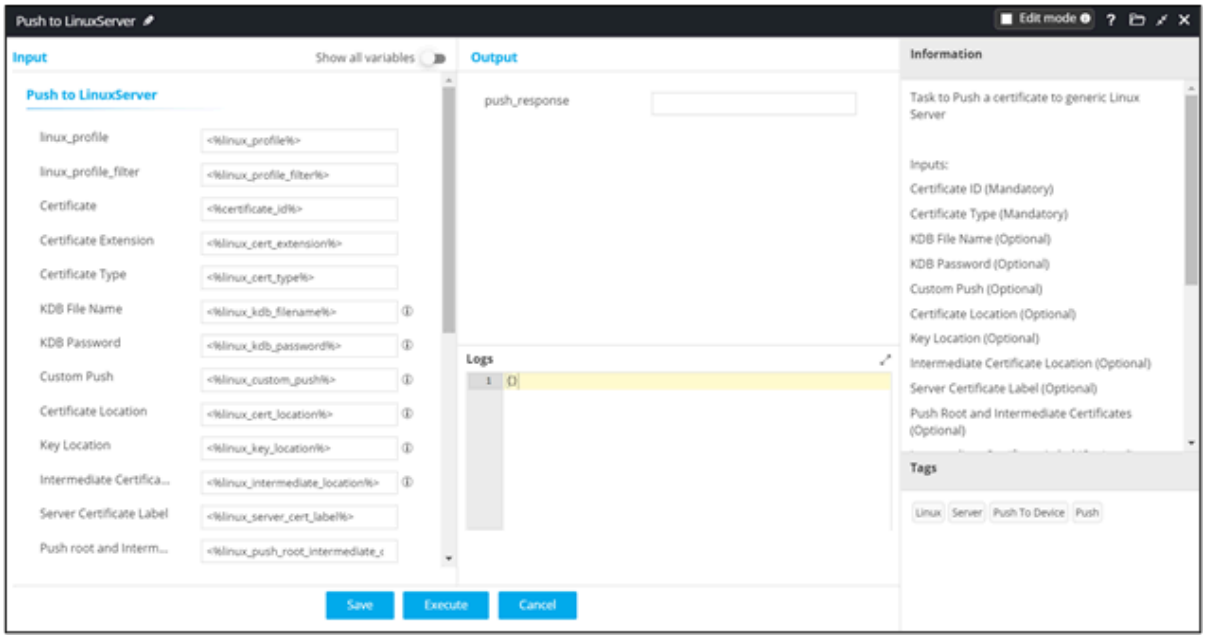
1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

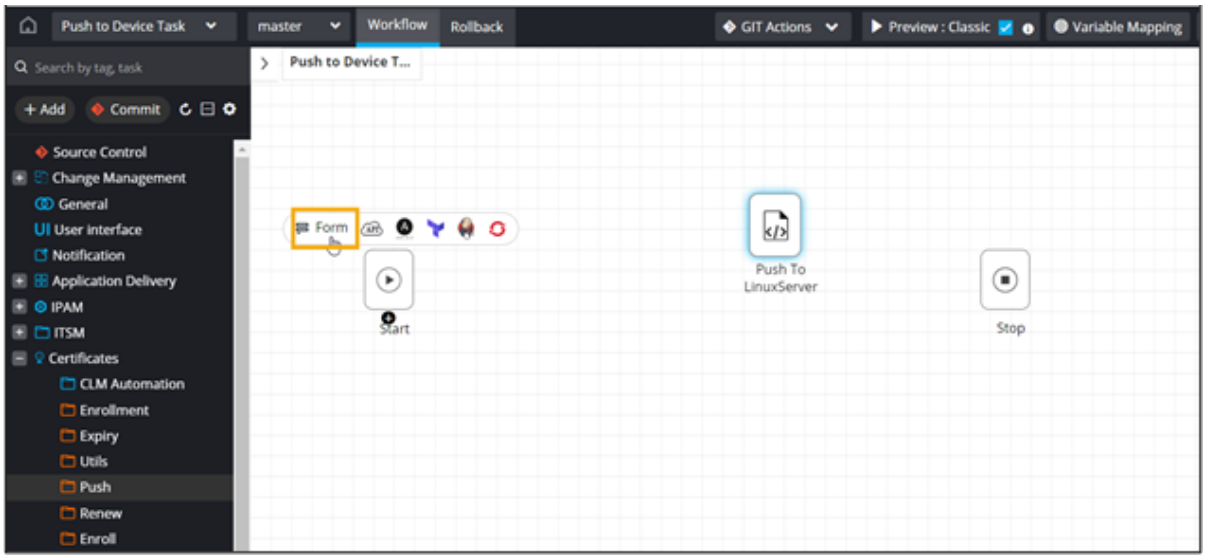


3. From the **Certificates** folder, click **Push**.
   The following tasks for pushing certificates are available in the **Push** folder:
   - Push to Apache Server
   - Push to F5 device
   - Push to Citrix Device
   - Push to IIS Server
   - Push to Linux Server
4. From the **Push** folder, drag and drop any of the Push tasks. For example, the **Push to Linux Server** task.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

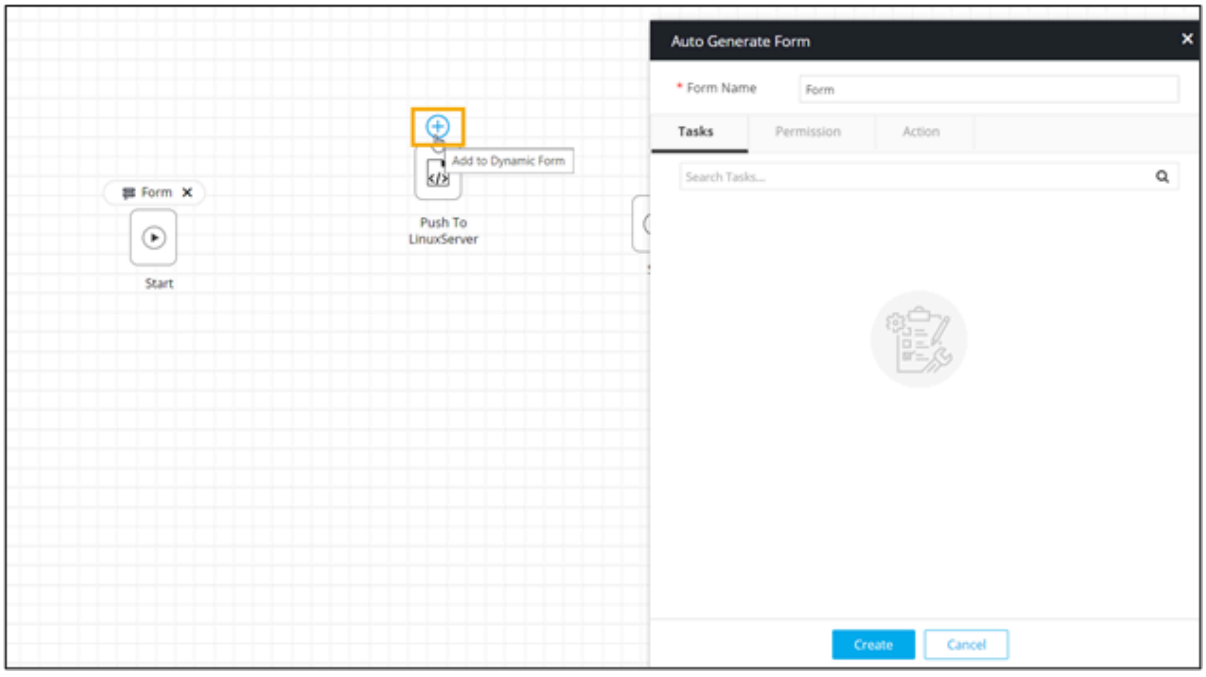


5. Click **Save**.
6. To auto-generate a form for this workflow, click **Form** above the **Start** task.



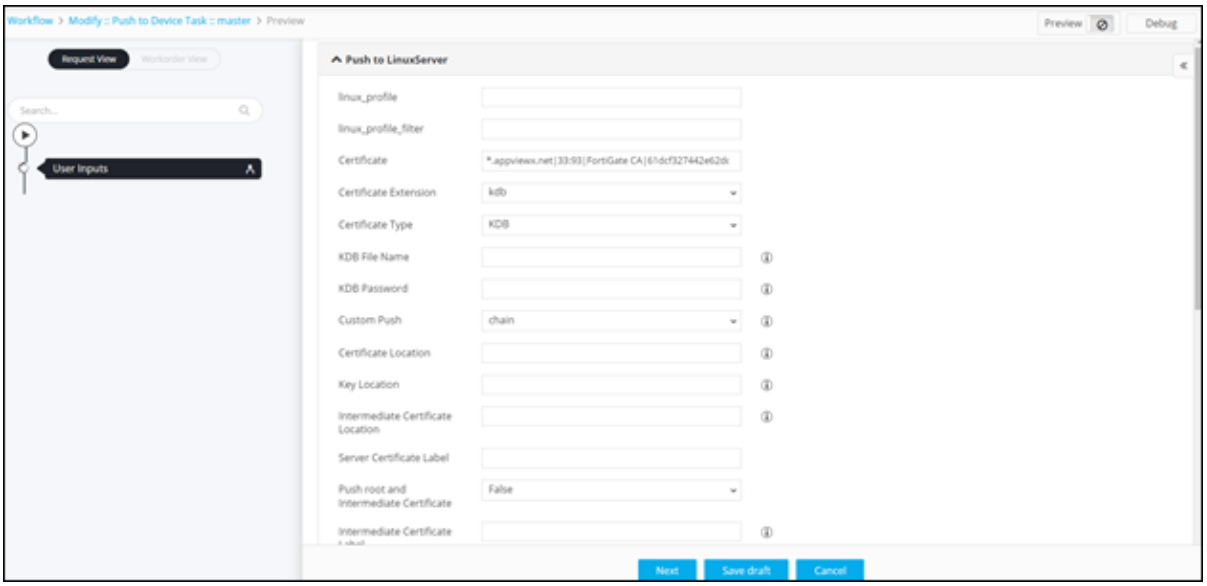
7. Click ⊕ above the **Push to LinuxServer** task to auto-populate the form fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



8. Select the fields required in the input form.
9. Provide a **Form Name** and click **Create**.
10. To view and download the certificate in a holistic view, from the **Utils** folder, drag and drop the **View and Download Certificate** prebuilt task.
11. To get a preview of the user input form, connect all the workflow tasks and click **Preview**.

    User Inputs form when the **Push to LinuxServer** task is selected is displayed.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: The fields displayed in the User Inputs form will vary depending on the Push task selected from the Push folder while designing the workflow.

Field Description for the User Inputs form

Field	Description
***Certificate Category**	Select the **Certificate Profile** from the following options: • **Server** • **Client** • **Code Signing** **Note: Server** is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note**: This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note**: Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note**: This field is displayed only when the **Auto Renewal** field is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	Add a description for the workflow, if required.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **Subject Alternative Name** from the options available in the dropdown.
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select the **IP Address** option in the **SAN** field.
Organization	Enter the name of the organization.
Organization Unit	Enter the name of the organization unit.
Locality	Enter the name of the locality in which the organization is situated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the Zip code in which the organization is located.
Email Address	Enter the Email Address of the organization.
***Validity Unit**	Select the **Validity Unit** from the options available in the dropdown.
***Validity Value**	Enter the **Validity Value** based on the Validity Unit selected.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown. **Note:** To retrieve the types of keys that can be availed, click .
***Bit Length**	Select the **Bit Length** from the options available in the dropdown.
Attribute	Select the **Attribute** from the options available in the dropdown.
Attribute Value	Enter the **Attribute Value** based on the Attribute selected.

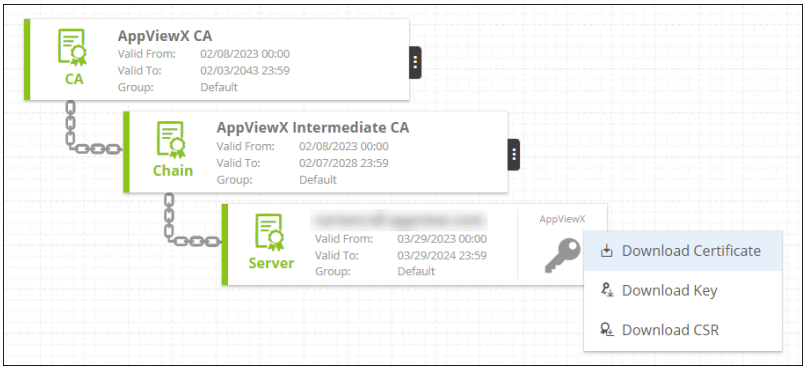
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
All Asterisk (*) marked fields are mandatory.	

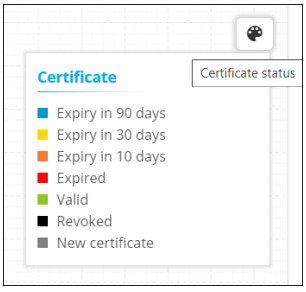
12. To add this attribute to the **Certificate Attributes** grid, click .
13. To edit the value of a particular attribute, select the attribute in the grid and click .
14. Enter the new value for the attribute in the **Value** field and click again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Click **Next**.

    Certificate created successfully.

19. To download the certificate, at the **View and Download Certificate** stage, hover your mouse over and from the options displayed, click **Download Certificate**.



20. Hover your mouse over to view the **Certificate status**.



Note: For more information on how to design custom workflows, refer to the Automation User Guide.

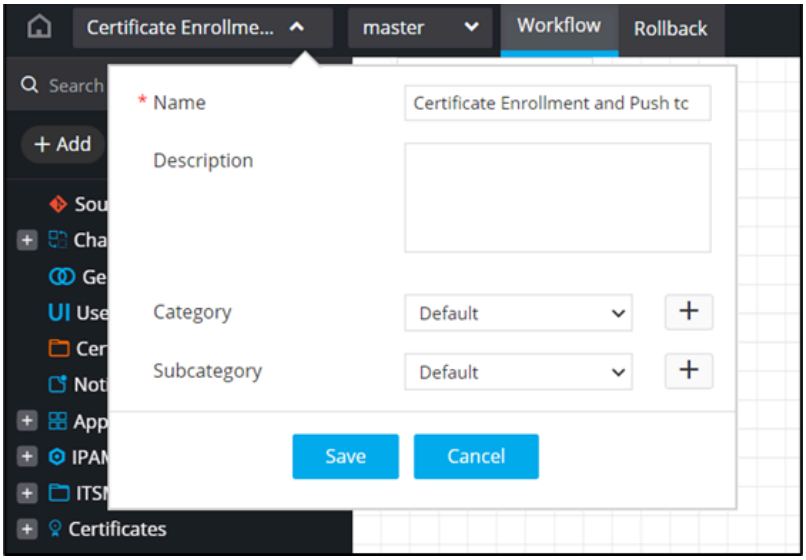
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Designing a Custom Workflow using OOB Tasks

You can use the OOB tasks and subflows available in the Automation module to build custom workflows for enrolling and renewing certificates. You can also add the OOB Push to Device subflow to push the certificates to a selected device.

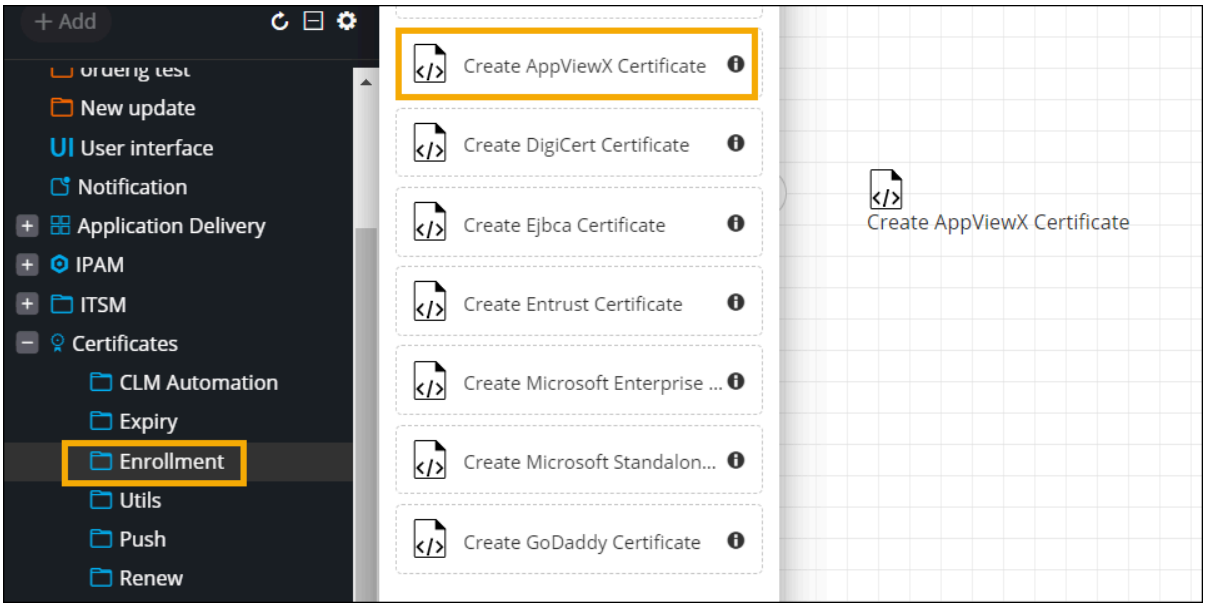
To design a custom workflow to enroll a certificate and push it to a device:

1. Navigate to the Workflow page in the **Automation** module and click **Create New**.
2. Enter a **Name** for the workflow and click **Save**.

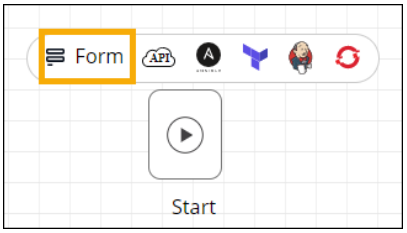


3. To access the OOB workflow tasks, from the left menu, click **Certificates**.
4. Under **Certificates**, from the **Enrollment** folder, drag and drop the required OOB task for enrolling a certificate, for example, the **Create AppViewX Certificate** task.

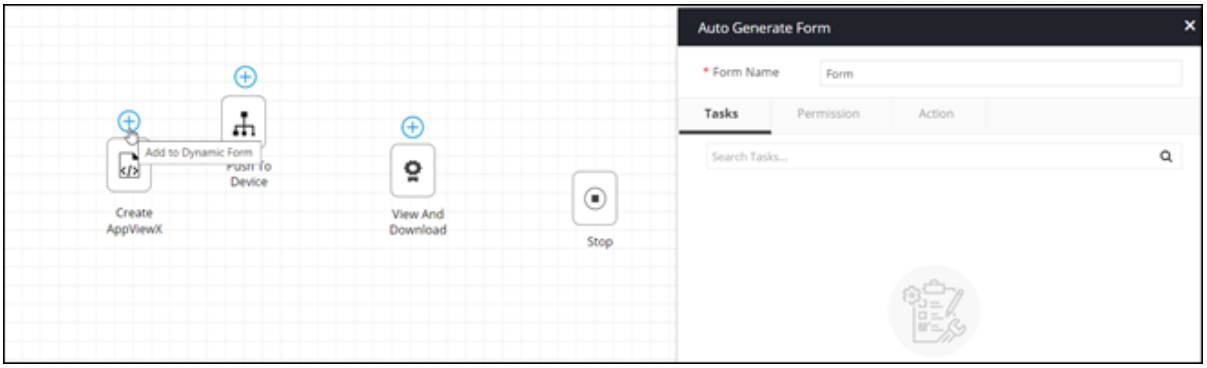
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. Click **Save**.
6. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **Push to Device** subflow.
7. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **View and Download Certificate** task.
8. To generate a form for this workflow, click **Form** above the **Start** task.



9. Click ⊕ above the **Create AppViewX Certificate** task to auto-populate the form fields.



10. Connect all workflow tasks and enable the workflow.
11. Trigger the workflow from the Request :: View/Run page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The workflow execution page is displayed with the workflow inputs requested at the first stage.

Field Description for the User Inputs form

Field	Description
***Certificate Category**	Select the **Certificate Profile** from the following options: • **Server** • **Client** • **Code Signing** **Note:** Server is the default selection.
***Certificate Group**	Select the **Certificate Group** from the options available in the dropdown.
***Certificate Authority**	Select the **Certificate Authority** from the options available in the dropdown. The following CAs are supported: • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX **Note:** This field is populated based on the **Certificate Group** selected.
***CA Account**	Select the **CA Account** from the options available in the dropdown. **Note:** This field is populated based on the **Certificate Authority** selected.
***Division**	Select the **Division** from the options available in the dropdown. **Note:** This field is displayed only when **DigiCert** is selected as the **CA**.
Certificate Type	Select the **Certificate Type** from the options available in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

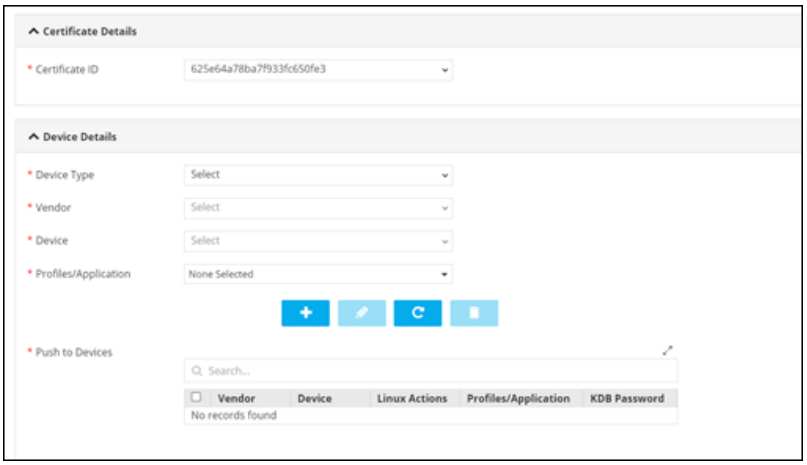
Field	Description
***Auto Renewal**	Select the required radio button to enable/disable **Auto Renewal**. **Note:** Default selection is set to **Off**.
Renew Before (Days)	Enter the number of days in the **Renew Before (days)** field. For example, if you enter 5, then the renewal request will be triggered 5 days prior to the expiry date. **Note:** This field is displayed only when the **Auto Renewal** field is enabled.
Description	Enter a description for the certificate to be created.
***Common Name**	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the **SAN** as either: • **DNS** • **IP Address**
DNS	Enter a valid DNS if you select the **DNS** option in the **SAN** field.
IP Address	Enter a valid IP Address if you select **IP Address** in the **SAN** field.
Organization	Enter the name of the organization with which the certificate will be associated.
Organization Unit	Enter the name of the organization unit with which the certificate will be associated.
State	Enter the name of the state in which the organization is located.
Country	Enter the name of the country in which the organization is located.
Zip Code	Enter the zip code.
Email Address	Enter the email address associated with the **Certificate Group**.
***Validity Unit**	Select the **Validity Unit** as either: • **Days** • **Months** • **Years**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity Value**	Enter a **Validity Value** based on the selected validity unit.
Challenge Password	Configure the **Challenge Password** to protect the certificate.
***Hash Function**	Select the **Hash Function** from the options available in the dropdown.
***Key Type**	Select the **Key Type** from the options available in the dropdown.
***Bit Length**	Select the **Bit Length** from the options available in the dropdown. **Note:** This field will be populated based on the selected **Key Type**.
Attribute	Select the **Attribute** from the available options.
Attribute Value	Enter a value for the selected attribute.
All Asterisk (*) marked fields are mandatory.	

12. To add this attribute to the **Certificate Attributes** grid, click .
13. To edit the value of a particular attribute, select the attribute in the grid and click .
14. Enter the new value for the attribute in the **Value** field and click again to update the value.
15. To delete a certificate attribute, select the attribute in the grid and click .
16. To maximize the **Certificate Attributes** grid, from the top right corner of the grid, click .
17. To search for a particular attribute in the grid, type the keyword(s) in the search field.
18. Click **Next**.
    AppViewX Certificate is created successfully.
19. At the **Device Inputs** stage of workflow execution, under **Device Details**, select the requested field information as described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



This table describes the field information in this section:

Field Description for Device Details section

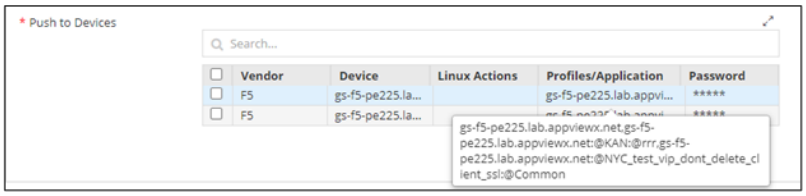
Field	Description
***Device Type**	Select the **Device Type** from the options available in the dropdown.
***Vendor**	Select the **Vendor** from the options available in the dropdown. **Note:** The vendor list is populated based on the **Device Type** selected.
***Device**	Select the **Device** from the options available in the dropdown. **Note:** The device list is populated based on the **Vendor** selected.
Linux Actions	Select the **Linux Action** from the options available in the dropdown. **Note:** This field is displayed only when you select **Linux Server** in the **Vendor** field.
***Profile/ Application**	Select the **Profile/Application** from the options available in the dropdown. **Note:** The **Profile/Application** list is populated based on the **Device** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB Password**	Configure a password to access the KDB file. **Note:** This field is displayed only when you select **Default** in the **Linux Actions** field.
***Push to Devices**	Add the selected profile/application to the grid as described below the table.
All asterisk (*) marked fields are mandatory.	

20. To add the selected profile/application to the grid, click .
    The **Profile/Application** is added to the **Push to Devices** grid.

Note: If you select multiple profiles/applications, they will be displayed in the **Push to Devices** grid, under the **Profiles/Applications** column as comma separated values.



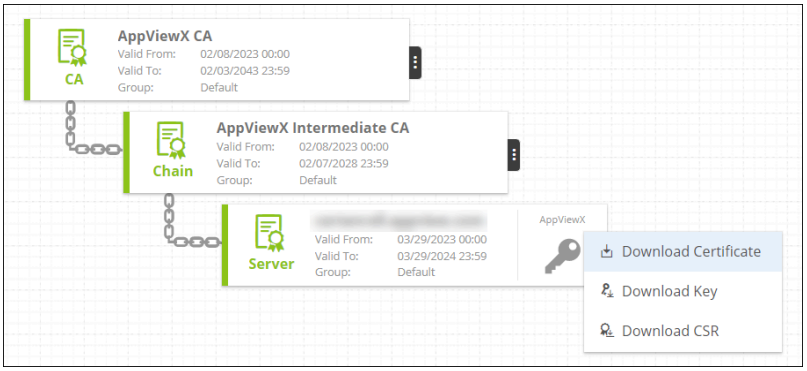
Actions available in the Push to Devices grid

Action	Description
	Allows you to edit the device details. You can do this by selecting the attribute in the grid, click , enter the new value for the attribute, and click again.
	Allows you to delete a profile/application.
	Allows you to maximize the **Push to Devices** grid.
Search bar	Allows you to search for a profile/application in the grid.

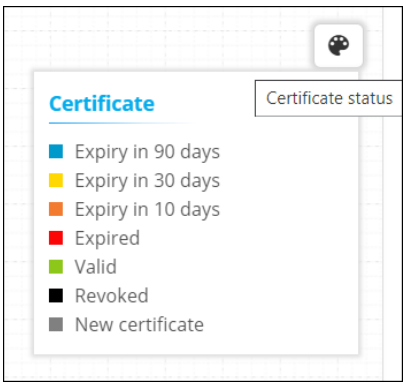
21. Click **Submit**.
    Certificate is pushed to the selected device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

22. To download the certificate, at the **View | Download Certificate** stage of the workflow, hover your mouse over , and from the options displayed, click **Download Certificate**.



23. Hover your mouse over to view the Certificate status.



Note: For more information on how to design workflows, refer to the Automation User Guide.

Scheduling an OOB workflow

You can also schedule these OOB workflows to be triggered at specific time intervals (once or repeat daily, weekly, monthly, yearly) as per your requirement.

Note: For more information on scheduling workflows, refer to the Automation User Guide.

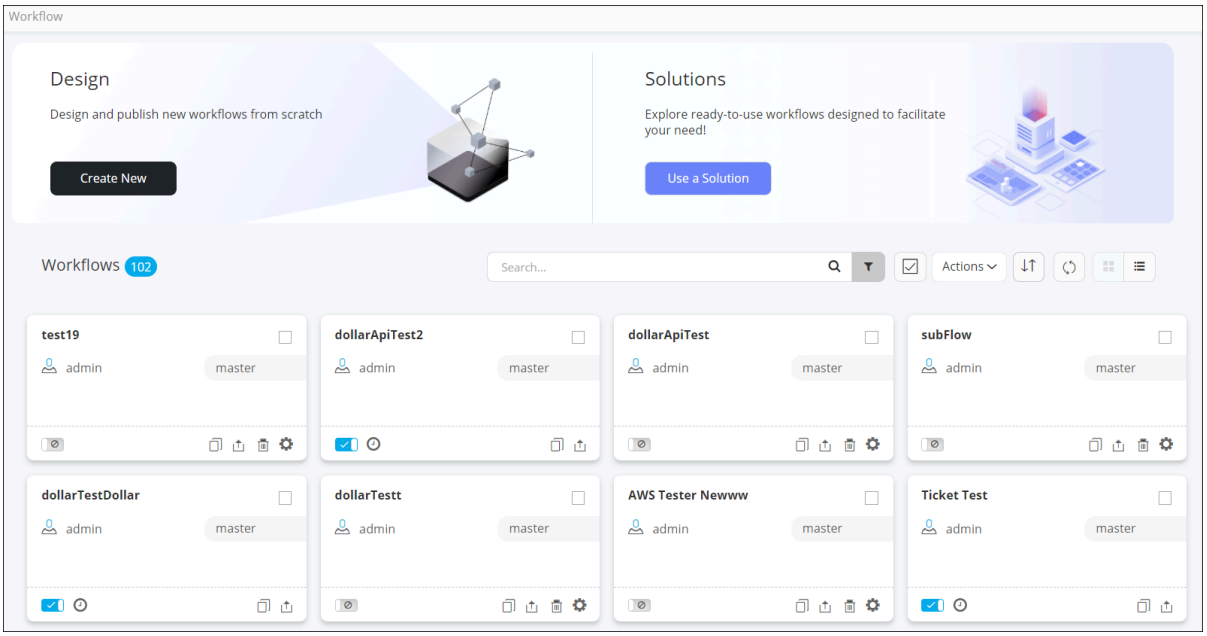
Customizing an OOB Workflow

You can customize any of these OOB workflows by modifying individual tasks within the workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To customize a workflow:

1. Navigate to the **Workflow** page in the **Automation** module.



2. On the **Workflow** page, search for the workflow you want to customize by typing the keyword in the search bar.
3. Disable the workflow by turning off the toggle on the workflow card.
4. Click on the workflow to open it in the design space.
5. Modify the required tasks.
6. Once the tasks have been modified as required, validate and enable the workflow.
7. Trigger the workflow from the Request :: View/Run page.

Managing Certificates Using AppViewX Terraform Provider

What is Terraform?

Terraform is an infrastructure-as-code tool that lets you build, change, and version cloud and on-prem resources safely and efficiently.

HashiCorp Terraform is an infrastructure-as-code tool that allows you to define both cloud and on-prem resources using human-readable configuration files. These files can be versioned, reused, and shared. Terraform enables you to apply a consistent workflow to provision and manage your infrastructure throughout its entire lifecycle. It can handle low-level components such as compute, storage, and networking resources, as well as higher-level components like DNS entries and SaaS features.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

How does Terraform work?

Terraform creates and manages resources on cloud platforms and other services through their application programming interfaces (APIs). Providers enable Terraform to work with virtually any platform or service with an accessible API.

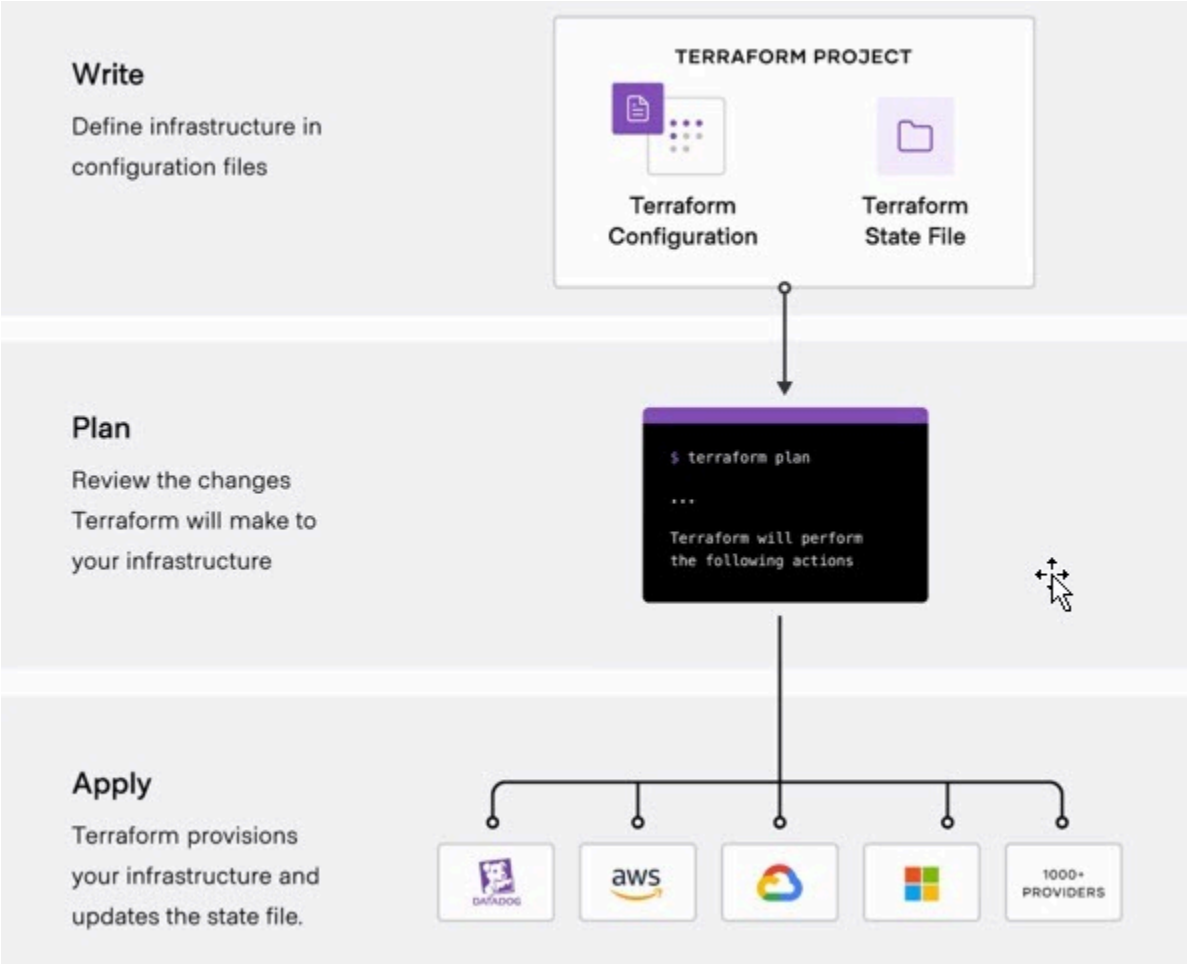
HashiCorp and the Terraform community have already written thousands of providers to manage many different types of resources and services. You can find all publicly available providers on the Terraform Registry, AppViewX Terraform is one of the providers.

The core Terraform workflow consists of three stages:

- **Write:** You define resources that span multiple cloud providers and services. For example, you can create a configuration to deploy an application on virtual machines within a Virtual Private Cloud (VPC) network, complete with security groups and a load balancer.
- **Plan:** Terraform creates an execution plan that outlines the infrastructure it will create, update, or destroy based on the existing infrastructure and your configuration.
- **Apply:** Once approved, Terraform executes the proposed operations in the correct sequence, aking resource dependencies into account. For example, if you update the properties of a VPC and change

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

the number of virtual machines within it, Terraform will re-create the VPC before scaling the virtual machines.



What AppViewX Terraform Provider does?

- Creates Certificate with the provided CSR Parameters.
- Downloads the certificate in different formats along with the trust store certificates, if needed
- Downloads the private key from AppViewX in password protected manner and in plain .pem format

Where is AppViewX Terraform Provider Hosted?

- The latest version of AppViewX Terraform Provider is 1.0.1 which is hosted in Hashicorp Terraform Registry.
- Opensource git hub repository which will be synced with this Terraform Registry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Authentication Models

- AppViewX user name and password credentials
- AppViewX service account credentials

Supported APIs and Details

Following are the APIs used internally in AppViewX Terraform Provider to create certificates and download them:

- Log onto AppViewX using your user name and password
  - Using the session id for further API calls
- Log onto AppViewX using service account credentials
  - Using the access token for further API calls
- Create Certificate with the provided CSR parameters in the .tf file.
  - Create Certificate uses Visual Workflow process, so disabling the approval level in policy will be helpful.
- Download end certificate in formats such as .pem, .crt, .cer, .der, .p12, .pfx, .jks.
  - Download trusted certificates along with .p12, .pfx and .jks formats.
- Download the private key created in AppViewX in the password protected manner or in plain .pem format
- OpenSSL command to get the plain private key from the password protected key:

```
openssl pkey -in <Password protected private key file> -out <Plain Private key file path> -passin pass:<Password of the private key>
```

How to use AppViewX Terraform Provider?

- Install and configure Terraform on your local machine where you intend to use it.
- Copy the provider from the AppViewX Terraform provider link and add it to your local version.tf file
- Create a .tf configuration file to enroll the certificate.
- Remove the .tfstate configuration:

```
rm -rf ./terraform.tfstate
```

- Validate the terraform configuration:

```
terraform validate
```

- Review the execution plan:

```
terraform plan
```

- Apply the Terraform configurations:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
terraform apply
```

Post this step, the certificate creation process will be triggered.

.tf file Parameters explained

#	Field Name	Field Type	Mandatory	Description	Sample
1	appviewx_username	String	No	User name of the AppViewX user to login and perform API calls.	test_user
2	appviewx_password	String	No	Password of the AppViewX user to login and perform API calls.	password
3	appviewx_client_id	String	No	Client ID of the AppViewX service account to login and perform API calls.	test_user
4	appviewx_password	String	No	Client secret of the AppViewX service account to login and perform API calls.	password
Note: Mandatorily provide username and password, or client ID and client secret.					
5	appviewx_environment_is_https	Boolean	Mandatory	Used to frame the AppViewX API URL.	true
6	appviewx_environment_ip	String	Mandatory	FQDN/IP address of the AppViewX instance for making API calls.	pe-cert-iot-150-192.lab.appviewx.net
7	appviewx_environment_port	String	Mandatory	Used to frame the AppViewX API URL.	31443

appviewx_create_certificate resource .tf file parameters

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Possible Values / Examples
1	common_name	String	No	CSR Parameter - Common Name	sample.test.com
2	dns_names	List of String	No	CSR Parameter - List of DNS names	[“sample.test.com”, "sample12.test.com”]
3	hash_function	String	No	CSR Parameter - Hash Function	Possible values: SHA256, SHA160, SHA224, SHA512, SHA384 **Note:** Values might vary based on the CA.
4	key_type	String	No	CSR Parameter - Key Type	Possible values: RSA, DSA, EC **Note:** Values might vary based on the CA.
5	bit_length	String	No	CSR Parameter - Bit Length	Possible values: 1024, 2048, 3072, 4096, 7680, 8192 **Note:** Values might vary based on the CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Possible Values / Examples
6	certificate_authority	Boolean	No	Used to frame the AppViewX API URL.	true
7	ca_setting_name	String	No	FQDN/IP address of the AppViewX instance for making API calls.	pe-cert-iot-150-192.lab.appviewx.net
8	certificate_type	String	No	Used to frame the AppViewX API URL.	31443
9	custom_fields	Object	No	AppViewX configured certificate attributes, which will be seen under Certificate Attributes column in certificate inventory,	{"request_by": "terraform"}
10	vendor_specific _fields	Object	No	Based on the CA, these values will go under Vendor Specific fields during the certificate enrollment of that particular CA.	{"templateName": "WebServer"}
11	validity_days	Integer	No	Certificate validity in days.	Possible values: 1 to 365

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Possible Values / Examples
12	validity_unit	String	No	Certificate validity type like days, months, or years	Possible values: days,months, years
13	validity_unit _value	Integer	No	Certificate validity based on the unit.	12
14	certificate_group _name	String	No	Certificate group name under which the certificates will be placed in AppViewX certificate inventory.	test_group1
15	is_sync	Boolean	No	• If sync is enabled, then the certificate is created and downloaded in the same API call. • If sync is disabled, then the certificate creation will be triggered. AppViewX Terraform will receive resourceId as response, which can	true

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Possible Values / Examples
				be used to download the certificate later.	
16	certificate_download_path	String	No	Path where the certificate content is to be downloaded.	Possible scenarios: • /home/sample/testcert • home/sample/ • testcert

Note: Following are the possible download paths applicable to both certificate and private key downloads:

1. /home/sample/testcert
   - AppViewX Terraform will first check if testcert is a folder. If it is, the certificate will be downloaded with the CN as the filename under the sample directory.
   - If testcert is not a directory but sample is, then the certificate will be downloaded with testcert as the filename under the sample directory.
   - If neither testcert nor sample are directories, a new folder named sample will be created, and the certificate will be downloaded with testcert as the filename inside the sample directory.
2. /home/sample/
   - If sample is a folder, the certificate will be downloaded with testcert as the filename inside the sample directory.
   - If sample is not a folder, a new folder named sample will be created, and the certificate will be downloaded with testcert as the filename inside the sample directory.
3. testcert
   - The certificate is downloaded with the CN as file name in the same working directory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Possible Values / Examples
17	certificate_download _format	String	No	Format in which the certificate will be downloaded.	Possible values: PEM, CRT, DER, CER, P12, PFX, JKS
18	certificate_download _password	String	Yes for P12, PFX and JKS formats.	Password used to download the certificates if they are in P12 or PFX or JKS formats.	password
19	certificate_chain _required	Boolean	No	If enabled, then the trust store certificates will be added to the end certificate during the download. **Note:** This is applicable only for P12, PFX and JKS certificate formats.	true
20	key_download _path	String	No	Path where the private key content is to be downloaded.	Possible scenarios: • /home/sample/testcert • home/sample/ • testcert

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Possible Values / Examples
21	key_download _password	String	No	Password to use to download the private key.	password
22	download_password _protected_key	Boolean	No	Private keys can be downloaded from AppViewX only in password protected manner. • If this flag is enabled, then the private key will be downloaded as an encrypted private key. • If disabled, then openSSL command is used to convert it into a plain private key and save it in the provided path.	false

appviewx_download_certificate resource .tf file parameters

#	Field Name	Field Type	Mandatory	Description	Sample
1	resource_id	String	No	Resource ID obtained in the previous appviewx_create_certificate resource response	6128381dq231sw1ww

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Sample
				log will be used to download the certificate post issuance.	

Note: If is_sync=false, then this resource can be used along with appviewx_create_certificate resource as shown:

```
....
....
}
resource "time_sleep" "wait" {
        depends_on = [appviewx_create_certificate.createcert]
        create_duration = "10s"
}
resource "appviewx_download_certificate" "downloadcert"{
 depends_on = [time_sleep.wait]
 resource_id=appviewx_create_certificate.createcert.resource_id
        .....
}
```

2	common_name	String	No	Common name of the certificate to download from AppViewX.	test.sample.com
3	serial_number	String	No	Serial number of the certificate to download from AppViewX.	12:QQ:23:12:34:45:45:23

Note: Mandatorily provide username and password, or client ID and client secret.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Sample
4	certificate_download_path	String	No	Path where the certificate content is downloaded.	Possible scenarios: • /home/sample/testcert • home/sample/ • testcert
5	certificate_download_format	String	No	Format in which the certificate will be downloaded Possible values: PEM, CRT, DER, CER, P12, PFX, JKS	PEM
6	certificate_download_password	String	Yes for P12, PFX and JKS formats	Password used to download the certificates if they are in P12 or PFX or JKS formats.	password
7	certificate_chain_required	Boolean	No	If enabled, then the trust store certificates will be added to the end certificate during the download. **Note:** This is applicable only for P12, PFX and JKS certificate formats.	true

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Field Name	Field Type	Mandatory	Description	Sample
8	key_download _path	String	No	Path where the private key content will be downloaded.	Possible scenarios: • /home/sample/ testcert • home/sample/ • testcert
9	key_download _password	String	No	Password used to download the private key.	password
10	download_password _protected _key	Boolean	Optional	Private keys can be downloaded from AppViewX only in password protected manner. If this flag is enabled then the private key will be downloaded as an encrypted private key. If disabled then openssl command is used to convert it to a plain private key and save it in the provided path	false

Sample Provider and Resources .tf files

Sample version.tf file

```
terraform {
  required_providers {
    appviewx = {
      source = "AppViewX/appviewx"
      version = "1.0.1"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  }
 }
}
```

1. Create the certificate in sync mode, which allows the certificate to be created and downloaded in a single `appviewx_create_certificate` resource.

```
resource "appviewx_create_certificate" "createcert"{
 common_name="sample.test.com"
 hash_function="SHA256"
      key_type="RSA"
      bit_length="2048"
      certificate_authority="Microsoft Enterprise"
      ca_setting_name="msca"
      #certificate_type="SSL Certificate"
      #dns_names=["test.com","test12.com"]
      custom_fields={"request_by":"terraform"}
      vendor_specific_fields={"templateName":"WebServer"}
      validity_unit=365
 validity_unit_value="years"
      certificate_group_name="cert_group"

      is_sync=true
      certificate_download_path="/home/sample/test/"
      certificate_download_format="P12"
      certificate_download_password="test"
      certificate_chain_required=true

      key_download_path="/test/testcert123"
      key_download_password="password"
      download_password_protected_key=false
}
```

2. Create a certificate in ASYNC mode, where certificate creation is triggered first, followed by a delayed certificate download using the `appviewx_download_certificate` resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
resource "appviewx_create_certificate" "createcert"{
 common_name="test.sample.com"
 hash_function="SHA256"
       key_type="RSA"
       bit_length="2048"
       certificate_authority="Microsoft Enterprise"
       ca_setting_name="msca"
       #certificate_type="SSL Certificate"
       #dns_names=["test.com","test123.com"]
       custom_fields={"request_by":"terraform"}
       vendor_specific_fields={"templateName":"WebServer"}
       validity_unit=365
 validity_unit_value="years"
       certificate_group_name="cert_group"
       is_sync=false
}

resource "time_sleep" "wait" {
  depends_on = [appviewx_create_certificate.createcert]
  create_duration = "10s"
}

resource "appviewx_download_certificate" "downloadcert"{
 depends_on = [time_sleep.wait]
 resource_id=appviewx_create_certificate.createcert.resource_id
       certificate_download_path="/Downloads/testcert123"
       certificate_download_format="P12"
       certificate_download_password="test"
       certificate_chain_required=true
       key_download_path="/test/testcert123"
       key_download_password="password"
       download_password_protected_key=false

}
```

3. Create a certificate in ASYNC mode, where certificate creation is triggered, and the user can later attempt to download the certificate at any time using the `appviewx_download_certificate` resource, either by common name and serial number or by resource ID.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
resource "appviewx_create_certificate" "createcert"{
 common_name="test.domain.com"
 hash_function="SHA256"
       key_type="RSA"
       bit_length="2048"
       certificate_authority="Microsoft Enterprise"
       ca_setting_name="msca"
       #certificate_type="SSL Certificate"
       #dns_names=["test.com","test123.com"]
       custom_fields={"request_by":"terraform"}
       vendor_specific_fields={"templateName":"WebServer"}
       validity_unit="years"
       validity_unit_value=2
       certificate_group_name="cert_group"
       is_sync=false

}

resource "appviewx_download_certificate" "downloadcert"{
 resource_id="564647657564gfdfx3w"
 common_name="test.domain.com"
 serial_number="21:23:123…"
       certificate_download_path="testcert"
       certificate_download_format="P12"
       certificate_download_password="password"
       certificate_chain_required=true
       key_download_path="/test/testcert123"
       key_download_password="password"
       download_password_protected_key=false
}
```

Troubleshooting

1. Ensure that the provider version is correct.
2. Verify that the fields in the `.tf` files have the exact field names and types.
3. Review the console logs after running the `terraform apply` command.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Change the logging level using the command: `export TF_LOG=DEBUG` or `export TF_LOG=TRACE`.
5. **For authentication-related errors:** Check the AppViewX user account's role and permissions in the AppViewX GUI to ensure the user has access to create and download certificates.
6. **For internal server errors:** Verify the provided input parameters and check the AppViewX server logs for any failures or issues on the AppViewX side.

Enhancements Implemented

1. The group name must be provided in the payload when creating the certificate.
2. Ability to enroll certificates from Sectigo CA.
3. Option to download the certificate and private key separately.
4. Support for using service account credentials alongside username and password.
5. Capability to pull updates directly from the AppViewX Terraform registry.
6. Enhanced logging in Terraform to display error messages from AppViewX for improved clarity.
7. Support for specifying certificate validity in days, months, and years.

Use Cases supported in AppViewX Terraform Registry v1.0.1

1. Custom attributes are functional, allowing users to view Terraform-issued certificates with the field `custom_fields={"fieldname":"value"}`.
2. After creating certificates with Terraform, the CA connector displays all relevant information, such as certificate type, CSR parameters, and template names.
3. Ability to issue certificates for MSCA, AppViewX CA, and CCM CA, all of which were tested in an internal lab.
4. Ability to create and download certificates in both async and sync modes.
5. AbleAbility to download the private key in both plain and password-protected formats.
6. When `validity_unit="days"` and `validity_unit_value=1`, the validity period is automatically calculated in days, months, and years are all supported for validity calculations.

Future Roadmap Items

• Support renewal before provided number of days.
• Improve logging for better handling of 407 Proxy Authentication Required errors.
• Ability to support multiple versions of AppViewX providers.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Points to Remember

- Users can authenticate using either username/password or client ID/client secret.
- Downloading the private key is optional but access to private key download in AppViewX is required to retrieve the key.
- Fields related to certificate download are mandatory when is_syncis true and within the appviewx_download_certificateresource.
- The `Certificate Password` field is only required for formats such as PFX, P12, and JKS.
- The `isChainRequired` field is applicable only for formats such as CRT, CER, CERT, PEM, and DER.
- Users on older versions of the provider should update their resource names to appviewx_create_certificate and appviewx_download_certificate. All other fields remain unchanged, allowing seamless usage.

Standard Practices

- PKI Standard Practices
- CLM - Best Practices
- Standard Practices followed in the Certificate Inventory Management
- Securing CERT+

PKI Standard Practices

Offline Root CA

- The root CA should never be connected to the network or to the domain and no fingerprint of the server should ever be recorded since the root key compromise will impact the entire PKI hierarchy.
- Root CAs should always stay offline and shut down except when signing the Issuing CA certificates and during root CRL publish.
- Access to the Root CA to sign the Issuing CA request should be initiated in an agreed and controlled workflow so as to not compromise the Root CA in any means.
- Once the Issuing CA certificate has been issued and Root CRL published the Root CA should be turned off.
- Ensure to publish a reasonably short-lived Root CA CRL, the recommendations from NIST is to have the Root CA CRL published for 1 year and ensure to renew the CRL before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- We strongly recommend that all your CA keys be stored securely in a FIPS 140-2 Hardware Security Module (HSM).
- Protect the server during boot using Bitlocker or any other encryption system of choice and ensure to backup CA private key, CA registry Key, the CA database, and the CA certificate.
- Ensure to enable an audit event to track all actions performed on the Root CA.

Inline with Compliance

- Ensure to have a CP and CPS created to suit the organization's needs and ensure the PKI infrastructure meets all standards and requirements with respect to the CP and CPS.
- Any changes or addition of features ensure to capture in the CP and CPS documents.
- Ensure to renew the CA certificates(Root and Subordinate) within half its lifecycle.
- Enterprise key and certificate security policies should align with the latest regulatory, industry-standard recommendations, and guidelines such as key storage, secure communication protocols (TLSv1.2), cryptographic algorithms (RSA-2048), and hashing algorithms (SHA-2).
- Enterprise security architects should constantly monitor security standard recommendations and periodically update the enterprise's security policy.
- Ensure all security events are audited and a periodic security audit is performed to validate the security adherences and metrics.
- Encourage short-lived certificates for all key usages.

CSR Generation Standardization

- A process must be defined across the enterprise to generate CSR that aligns with the security standards and to store keys securely.
- Harden parameters such as Country and Organisation in accordance with organizational requirements.
- Access to keys should be restricted to authorized personnel.
- Key Generation, Certificate Request, and Approval processes should be well defined.

Archival

Signing keys do not require archival. We can always generate new keys for signing since the signed data is not encrypted. But encryption keys have to be archived so that the encrypted files during the certificate validity can be decrypted even after the certificate expiry. Also, this is recommended for security audits.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Secure Storage of Keys

- It is recommended to store private keys in HSM.
- Ensure respective certificate owners or certificate authorized administrators are granted access to private keys using the RBAC solution.
- Best practices training can be provided to certificate users and administrators to keep private keys secure.

Compromised CA/CA keys

- Ensure to discover a compromise as quickly as possible by implementing tracking and detection mechanisms and performing regular manual operational sanity checks.
- Establish well-defined communications plans for informing subjects, relying parties, and other stakeholders with sufficient details about the type of compromise so these parties can implement the appropriate remedial actions.
- If a CA system or signing key compromise occurs, the organization should perform the following steps:
  - Ensure that certificates issued to the organization’s systems or users from the compromised CA are revoked.
  - Notify all owners of the affected certificates about the CA compromise and establish a point of contact for responding to questions and providing guidance and instructions.
  - Replace all certificates from the compromised CA with new certificates from a different CA effective immediately.
  - Ensure that all relying parties have the certificate trust chains required to validate certificates from the new CA.
  - Ensure that revocation checking is enabled on all relying party systems.
- If the compromised CA is a root CA, the root certificate must be removed from all trust stores and relying on party systems.

Compromised Certificate Handling

- Ensured to be prepared to respond in a timely manner in case of a CA or end-entity certificate compromise and have a plan or workflow to replace all affected certificates or the trust chain.
- In the event of a key or certificate compromise, a fresh key pair should be generated on a secured system. The compromised item should be revoked and taken out of the service as soon as the systems are secured.
- If you are not sure of your private key possession, report it to your CA and suspend the key immediately. Once you find the key is secure, reinstate the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Compromise and Remediation Matrix

S/No.	Issue Type	Revoke compromised/ counterfeit certificates	Revoke CA certificate	Replace all certs issued	Remove/Revoke Root certificate
1	Impersonation	Yes	NA	NA	NA
2	RA compromise	Yes	NA	NA	NA
3	CA system compromise	NA	Yes	Yes	Yes
4	CA key compromise	NA	Yes	Yes	NA
5	Root CA compromise	NA	NA	Yes	Yes

CLM - Best Practices

Risks Involved in an Enterprise without CLM and their Solutions

S/No	Risks Involved in an Enterprise without CLM	Solutions
1	No centralized management for all certificates in an enterprise and to know the certificate's location.	Different modes to discover existing certificates along with the discovery source.
2	Enforcing teams to follow the enterprise security standards.	• Get information about all certificates within an enterprise. • Run a validation for the existing certificate against the organization's security standard.
3	Poor monitoring of certificate validity causes outages due to expired certificates.	• Continuous monitoring of the certificate status and notifications. • Automated renewals and provisioning should be available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

S/No	Risks Involved in an Enterprise without CLM	Solutions
4	Control over the generation of keys.	Provide a mode of access to teams to access and generate certificates for their requirements.

- Create a certificate lifecycle management action plan
- Start automating the certificate management process wherever feasible.
- Identify and expose all the neglected certificates, these are the certificates that will cause more damage during expiry.
- Ensure proper RBAC controls and avoid using direct user accounts and instead use identified admin accounts for access and control.
- Enable notifications and alerts to ensure timely renewal.
- Schedule scans to run overnight or after business hours.

Standard Practices followed in the Certificate Inventory Management

- Certificate Group
- Access Control
- Recommended Columns to View in the Default Inventory

Certificate Group

- Group similar certificates into logical groups
- Groups can be based on business units or teams using certificates
- Provide group owner details during configuration for easy tracking
- Create hierarchy-based grouping to leverage alert escalation on OOB workflow.
- Try and maintain the same policy across a hierarchy of groups. It is also allowed to set a different policy for each hierarchy.

The best way to manage certificates is to group certificates based on the following:

- AD Security Group vs Department
- Test vs Production
- Internal vs External Hierarchy
- Auto-renew vs Approved CSRs
- Auto Push Updated Certificate vs Controlled Push Updated Certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Access Control

Based on certificate groups, you can create resources and map devices/applications.

Identify various authorization roles that have to be created. Find the list of roles below:

- Certificate Administrator Team
- CERT Owner/Requester
- Approver
- Certificate Manager
- Inventory View

The certificate admin team should be granted access to view the entire certificate inventory and end-users should be able to view their respective certificates.

All managed/monitored certificates should be available on a single window for tracking and visibility. The product provides various columns that have rich information that might not be needed in all scenarios.

Recommended Columns to View in the Default Inventory

- Subject Distinguished Name (DN)
- Subject Alternative Names (SANs)
- Issue Date (not Before date)
- Expiry Date (not After date)
- Issuing Certificate Authority
- Key Length
- Key Algorithm (RSA, ECDSA)
- Signing Algorithm
- Validity Period (From the not Before date/time to the not After date/time)
- Installed location(s) of a certificate (IP or DNS address and file path)
- Certificate Owner (The group responsible for the certificate)
- Contacts (The group of individuals is notified of issues)
- Approver(s) (parties responsible for reviewing issuance and renewal requests)

As the inventory is a RegEx-based search engine, users can search for a certificate based on any parameter with various filters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Securing CERT+

CERT+ Certificate Lifecycle Management (CLM) offers capabilities to discover and manage certificates on devices and self-service certificate enrollment for users. CERT+ also acts as a Key Escrow for keys discovered and enrolled.

Typically, the private keys are stored by the devices handling SSL termination, and an SSL management tool retrieves them during certificate renewal. The tools and devices store them in their storage in the original format, which can be reused. If there is an attack on the device or tool storage, the private keys will be given away, which can be used to host an array of attacks.

AppViewX stores the private keys discovered in a secure part of the database, which is encrypted using the AES-256 algorithm. It encrypts each private key with independent keys and stores the encrypted independent keys in the database with a randomly generated key.

Thus, even if the hackers get the database, they will not be able to get the private keys. Only a maze of jumbled up characters will be visible to them, which does not make any sense and hence, rendering the attack useless.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 3: CERT+ Admin Guide

AppViewX CERT+ Admin Guide provides comprehensive instructions for administrators to efficiently manage and configure the CERT+ certificate lifecycle management solution. It covers key administrative tasks, including setup, and configuration, to ensure optimal performance and security of digital certificates.

As an admin user, you can perform the following tasks:

- Deploy and manage CERT+ hosts and licenses.
- Configure user accounts, authorization, and authentication.
- Monitor the system health of managed hosts and the application.
- Auto enroll certificates by automating all the steps involved, including CSR generation, domain ownership verification, certificate download, and provisioning, making the process efficient, scalable, and secure. (See Auto Enrollment Protocols)
- Onboard Certificate Authorities (CAs). (See Configuring CA Settings)
- Enforce organization standards by configuring certificate policies in **CERT+**. Thus the attributes of discovered certificates are compared against the certificate policy to ensure they are complaint. (See CA Policy)
- Configure certificate groups. (See Configuring Certificate Groups)
- Manage server devices. (See Configuring and Managing Servers)
- Manage firewall devices. (See Configuring and Managing Firewalls)
- Manage cloud devices. (See Configuring and Managing Cloud Devices)
- View certificate reports. (See Certificate Reports)

- Configuring CA Settings
- CA Policy
- Configuring Certificate Groups
- Configuring Certificates
- Configuring and Managing Devices
- Certificate Reports
- Auto-Enrollment Protocols
- MDM Device Integration for Certificate Lifecycle Management
- Configuring General Settings
- Appendix A: Prerequisites for Enabling the Integrated Windows Gateway Mode

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Appendix B: List of Scheduled Jobs
- Working with the Job Scheduler

Configuring CA Settings

- Amazon and Amazon Private CA
- CSC Global CA
- Custom CA
- DigiCert CA
- DigiCert MPKI
- DigiCert One
- EJBCA
- Entrust CA
- Entrust MPKI
- Futurex
- GlobalSign MSSL CA
- GlobalSign Atlas CA
- GlobalSign SSL CA
- GoDaddy CA
- Google CA
- HashiCorp Vault CA
- HydrantID CA
- IDnomic CA
- InCommon CA
- Let’s Encrypt CA
- Microsoft Enterprise CA
- Microsoft Standalone CA
- Nexus CA
- Sectigo CA
- SwissSign CA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Symantec CA
- Trustwave CA

Amazon and Amazon Private CA

Prerequisites

The prerequisites for configuring Amazon CA or Amazon Private CA account in AppViewX are as follows:

- An Amazon account for a user having necessary access for enrolling the certificates and other CLM operations.

  For links to detailed instructions for retrieving the above information, see the **References** section.

- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Refer to the section Managing Proxy Settings in the Platform guides.
- Policy JSON for AWS EC2 Instance Certificate Management.
- Prerequisite permissions for Amazon CA:

Policy JSON for EC2 Certificate Management

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "ssm:SendCommand",
    "ssm:DescribeDocument",
    "ec2:DescribeInstances",
    "ec2:DescribeRegions",
    "s3:ListBucket",
    "ssm:CreateDocument",
    "ssm:GetCommandInvocation",
    "s3:GetObject",
    "s3:ListAllMyBuckets",
    "ssm:DescribeInstanceInformation",
    "ssm:GetDocument",
    "s3:DeleteObject",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "s3:GetBucketLocation"
    ],
    "Resource": "*"
   }
 ]
}
```

Policy JSON for Certificate Management in AWS Classic and Application Load Balancers

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetServerCertificate",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:DescribeListeners",
    "acm:GetCertificate",
    "ec2:DescribeRegions",
    "elasticloadbalancing:DescribeTargetHealth",
    "acm:ImportCertificate",
    "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
    "iam:UploadServerCertificate"
   ],
   "Resource": "*"
  }
 ]
}
```

Policy JSON for AWS Cloudfront Certificate Management

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "Action": [
      "ec2:DescribeRegions",
      "cloudfront:ListDistributions",
      "cloudfront:UpdateDistribution",
      "cloudfront:GetDistributionConfig"
    ],
    "Resource": "*"
  }
 ]
}
```

Policy JSON for IAM Certificate Management

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetServerCertificate",
    "iam:UpdateServerCertificate",
    "iam:ListServerCertificates",
    "ec2:DescribeRegions",
    "iam:UploadServerCertificate"
   ],
   "Resource": "*"
  }
 ]
}
```

Policy JSON for ACM Certificate Management

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "acm:DescribeCertificate",
      "acm:RequestCertificate",
      "acm:GetCertificate",
      "ec2:DescribeRegions",
      "acm:ListCertificates",
      "acm:ImportCertificate"
    ],
    "Resource": "*"
  }
 ]
}
```

- Prerequisite permissions for Amazon Private CA

Policies and Permissions required for AWS IAM User

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "s3:PutObject",
    "s3:GetObjectAcl",
    "s3:GetObject",
    "s3:PutObjectAcl"
   ],
   "Resource": [
    "arn:aws:s3:::<bucketname>",
    "arn:aws:s3:::<bucketname>/*"
   ]
  },
  {
   "Sid": "VisualEditor1",
   "Effect": "Allow",
   "Action": [
    "acm-pca:GetCertificate",
    "ec2:DescribeRegions",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:RevokeCertificate",
      "acm:RenewCertificate",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:CreateCertificateAuthorityAuditReport",
      "s3:ListAllMyBuckets",
      "acm:DescribeCertificate",
      "acm-pca:IssueCertificate",
      "acm:RequestCertificate",
      "acm:GetCertificate",
      "acm:ListCertificates",
      "acm-pca:DescribeCertificateAuthority"
    ],
    "Resource": "*"
   }
 ]
}
```

AWS Simple Storage Service (S3) Bucket Policy for parsing Audit log

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "Service": "acm-pca.amazonaws.com"
   },
   "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation"
   ],
   "Resource": [
    "arn:aws:s3:::bucket_name/*",
    "arn:aws:s3:::bucket_name"
   ]
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  }
 ]
}
```

Prerequisites for Using a CyberArk Credential List for Onboarding

If credentials for onboarding have to be fetched from a credential list in CyberArk:

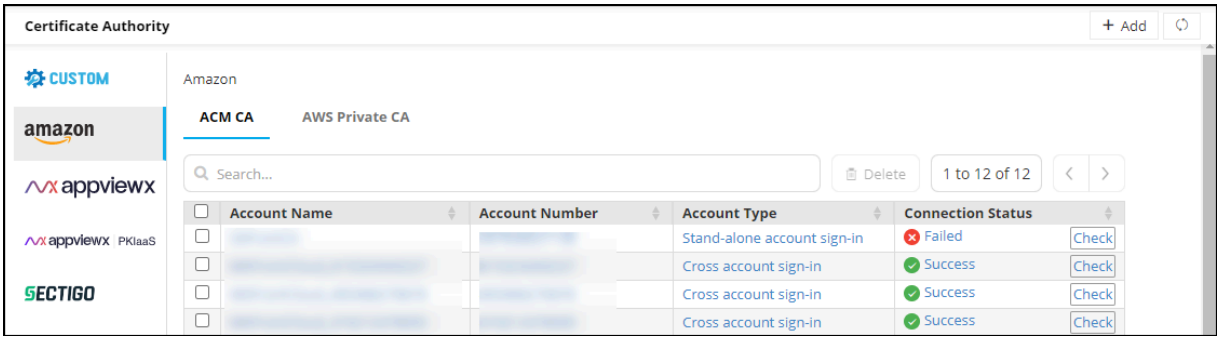
- Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

> **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

- Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Configuring Amazon CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Amazon**.
   The **Amazon** home page is displayed.



3. To configure Amazon CA, click **ACM CA** from the home page.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.

> **Note:** The **Configure Now** option is displayed if you are configuring a CA for the first time.

   The **Amazon** configuration page is displayed.
5. Enter/Select the following details in the **General Information** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Field	Description
***Account Type**	From the dropdown list, select one of the following account types: • **Standalone** (Traditional access key- and secret key-based communication) • **Cross or Federated** (Authentication using assume role)
***Account Name**	Enter your AWS account name.
***Account Number**	Enter your AWS account number.
Account Description	Enter any additional information related to your AWS account.
***Purpose/Usage**	From the dropdown list, select the certificate type(s) for which CLM actions will be enabled. **Possible values**: Server, Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
***Default Region**	Default region for API communication
***Data Center (AppViewX's CA agent)**	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

6. Enter/Select the following **Credentials**-related information.

Credentials - Field Description Table

Field	Description
Credential type*	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the CA setting. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
*: *Mandatory fields*	

7. Enter/Select the following details in the **Discover resources** section:

Discover Resources - Field Description Table

Field	Description
***Role ARN for Resource Discovery**	This field is displayed only when **Account Type** is **Cross or Federated**. To let the master account assume role for the child account (get temporary privileges to discover resources from the child account), configure the role ARN for resource discovery: a. Click (Settings). b. Enter the following details:

Field	Description
Role Session name	**Role Session name** is an identifier for the assumed role session. Use the **Role Session name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) **Default**: 3600 seconds (1 hour)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td>*Service Region</td><td>To select a service region:
a. To fetch the service regions for the account information provided, click Fetch Region.

The retrieved service regions are populated in the Select the Region(s) dropdown list.
b. From the Select the Region(s) dropdown list, select the required service region.</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Cert Sync**	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic schedule-based synchronization: a. For **Auto Sync**, select the **Yes** checkbox. b. For **Schedule based discovery**, use the two dropdown lists to select a duration. For example, to schedule the auto sync after every 2 days, from the first dropdown list, select **2** and from the second dropdown list, select **Days**. By default, the auto sync is set to **1 Hours**. **Note:** The **Schedule based discovery** dropdown lists are displayed only when **Auto Sync** is enabled.
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle. **Important:** If Route53 has been configured for any of the older Amazon Public CAs, ensure that, after migration, the zones are manually updated.
*: *Mandatory fields*	

8. Click **Save**.

   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully

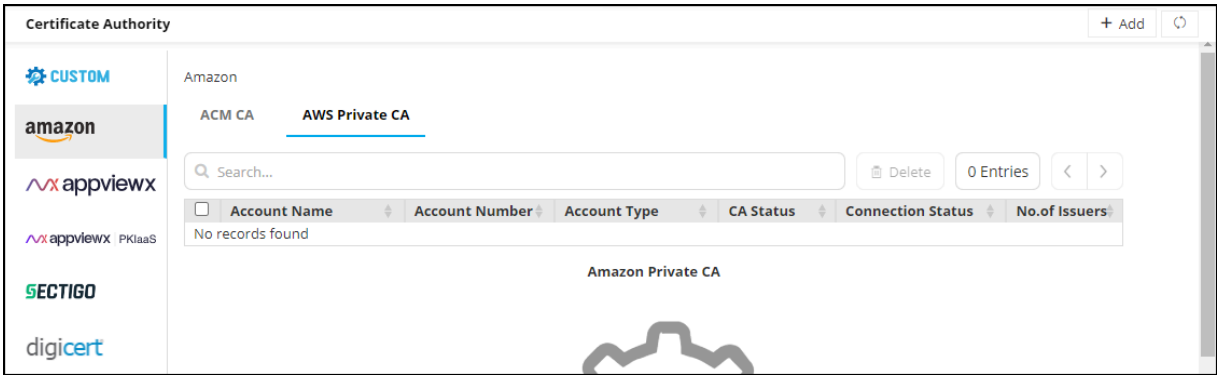
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Configuring Amazon Private CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Amazon**.
   The **Amazon** home page is displayed.
3. To configure the Amazon Private CA, click **AWS Private CA**.



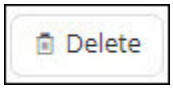
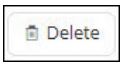
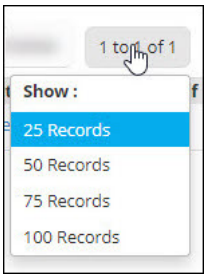
The **Amazon** home page is updated to display the inventory grid as shown in the image. In the inventory grid for the Amazon Private CA, master and child account details are logged as separate entries, instead of having just one master entry.

Fields in the inventory grid are explained in the table below:

AWS Private CA - Screen Description Table

Field	Description
Search	Use the **Search** field to search for accounts, by entering the value of one of the details listed in the inventory grid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To delete one or more accounts: a. From the inventory grid, select the checkbox corresponding to the account(s) you want to delete. b. Click  (Delete) . **Tip:** To delete all accounts listed in the inventory grid, select the checkbox in the grid header.
	To set the number of records that should be displayed on one page: a. Click . b. From the **Show** menu displayed, select the required value. 
	If the inventory grid spans more than one page, use this control to navigate the pages, one page at a time.
Account Name	This is the unique name for the Certificate Authority (CA) account entered at the time of account creation.
Account Number	AWS account number
Account Type	**Multi account**: Indicates that the account is a cross account **Single account**: Indicates that the account is a standalone account
CA Status	For an account, after all configuration details for Amazon Private CA are entered, you will be required to click the **Fetch issuer and save** button to sync and discover the issuers and the respective certificates for that account. The **CA Status** field shows the current status of this sync and discovery process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Possible values for this field are: • Completed • In progress **Note:** An account entry in the grid will be disabled till the **CA Status** is **In progress**.
Connection Status	To validate if connection has been established with the CA, click **Check**. If a connection has been established, this field is updated to display **Success** or **Failure**.
No. of Issuers	This field displays the number of issuers associated with the account. **Note:** For a master account, this field will show the number of issuers associated with only the master account. The value does not include the number of issuers associated with the child account.
*: *Mandatory fields*	

4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively. The **Amazon** page is updated to display fields for entering the CA configuration-related information.
5. On this screen, enter the following **Basic Information**:

Basic Information - Field Description Table

Field	Description
***Account type**	From the dropdown list, from the following options, select the customer's AWS account type: • **Standalone**: The user account and the resources are available in the same account. • **Cross or Federated**: Resources are available across multiple accounts and users are given role-based access.
***Account name**	Enter a unique name for the Certificate Authority (CA) account that will be used during certificate enrollment and policy creation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Account number**	Enter the customer's AWS account number.
Account Description	Enter any additional details related to the account, if required.
***Purpose/Usage**	From the dropdown list, select the purpose of the certificate that can be requested using this account.
Proxy Required	To allow all communication to the Certificate Authority (CA) to use the proxy details (provided in general settings; refer the CLMaaS Platform User Guide for more details), select this checkbox.
***Default Region**	From the dropdown list, select the default region for API communication.
Data Center (AppViewX's CA Agent)	From the dropdown list, select the data center that will be used to establish communication with the Certificate Authority (CA)
*: *Mandatory fields*	

6. Enter the **Credentials**-related information for the CA integration.

Credentials - Field Description Table

Field	Description
Credential type*	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the CA setting. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
*: *Mandatory fields*	

7. In the **Discover resources** section, enter the following details:

Discover Resources - Field Description Table

Field	Description
Role ARN for Resource Discovery*	This field is displayed only when **Account Type** is **Cross or Federated**. To let the master account assume role for the child account (get

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>temporary privileges to discover resources from the child account), configure the role ARN for resource discovery:
a. Click (Settings).
b. Enter the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you</td></tr>
</table></td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>assume an IAM role or federate a user in AWS STS.

To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td>Service Region*</td><td>Service regions are regions that are supported by the selected service.

To select a service region:
a. To fetch the service regions for the account information provided, click Fetch Region.The retrieved service regions are populated in the Select the Region(s) dropdown list.
b. From the Select the Region(s) dropdown list, select the required service region.</td></tr>
<tr><td>CA Operation Mode*</td><td>From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority:
• ACM Private CA
• AWS Certificate Manager (ACM)</td></tr>
<tr><td>S3 Bucket*</td><td>This field is displayed only when the ACM Private CA operation mode is selected. Enter the S3 bucket name.</td></tr>
<tr><td>Role ARN for S3 Bucket</td><td>This field is displayed only when the ACM Private CA operation mode is selected for a Cross or Federated account.
a. Click (Settings).

The ARN Advanced Settings action pane is displayed.</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>b. In the ARN Advanced Settings action pane, enter the following details:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
c. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td>CA Sync*</td><td>Select from one of the following options:
• Managed: AppViewX will connect with the customer’s AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
• Monitored: AppViewX will connect with the customer’s AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
• Ignored: AppViewX will connect with the customer’s AWS account but certificate discovery will be disabled.</td></tr>
<tr><td>Auto Sync</td><td>To enable/disable automatic synchronization, use the Auto Sync key.</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If **Auto Sync** is enabled, to set the frequency of the schedule-based sync: a. From the first dropdown list, select the interval between two schedule-based syncs. b. From the second dropdown list, select a unit for the interval (**Hours**/**Days**). For example, to set the frequency of the schedule-based sync to every 2 hours, from the first dropdown list, select **2** and from the second dropdown list, select **Hours**.
*: *Mandatory fields*	

8. Click **Fetch issuer and save**.
   - AppViewX will now discover all the Private CA Certificate Authorities across the selected region(s).
   - The inventory grid on the Amazon CA home page will be populated with the properties and details retrieved from this discovery.
   - The connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

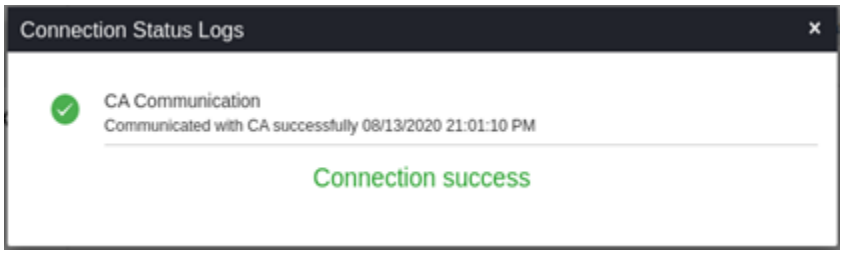
> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Amazon CA and Amazon Private CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Amazon**.
   The **Amazon** home page is displayed.
3. On the **Amazon** home page, select **Amazon** or **Amazon Private CA**.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **connection status** will be displayed as either **Connection success** or **Failure**.



References

Vendor documentation for retrieving the Amazon CA and Amazon Private CA configuration prerequisites:

- Creating an AWS account
- Creating an IAM user in your AWS account
- Managing access keys for IAM users

CSC Global CA

Prerequisites

The following values are required to configure the CSC Global CA:

- CA Base URL (the value is available in the UI field of the CA setting page)
- API Key
- Token

  Please contact the CSC Global team for retrieving the above listed prerequisite values.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

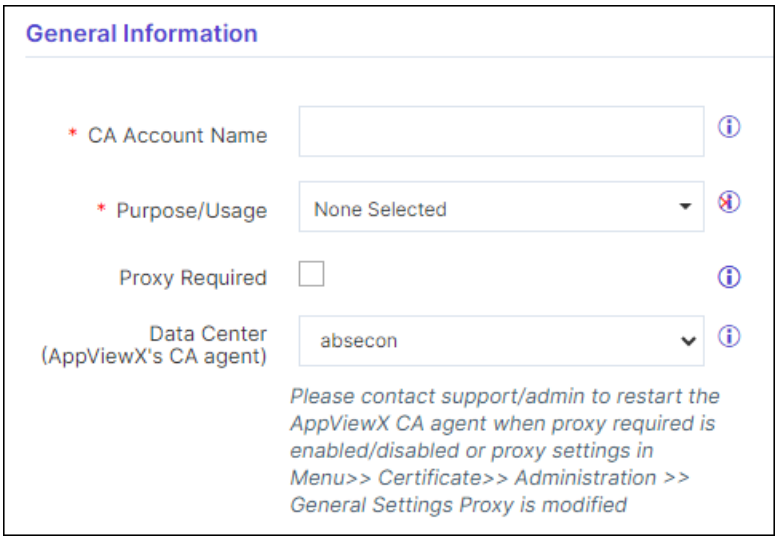
Configuring CSC Global CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **CSC**.

   The **CSC** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.

   The **CSC Global CA** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

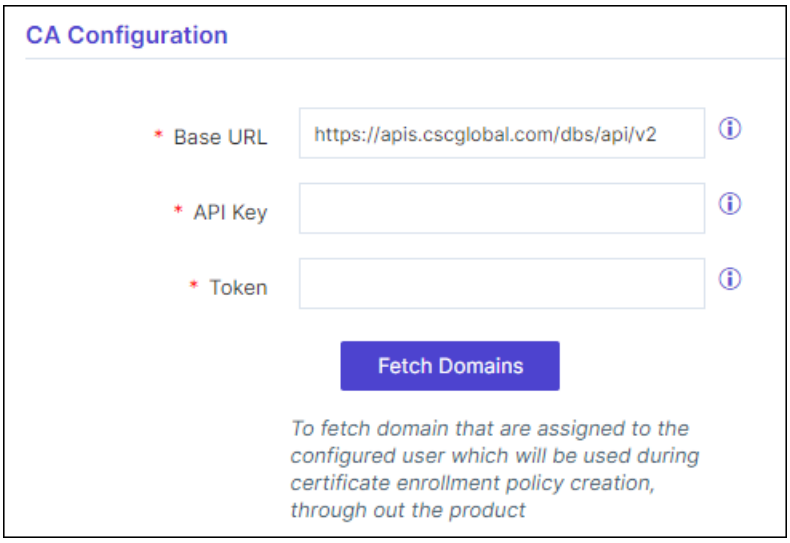


General Information - Field Description Table

Fields	Description
***CA Account name**	Enter a unique name in the text field to identify the CA account and be represented during certificate enrollment and policy creation. No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Select the purpose of the certificate from the dropdown list for which CLM actions will be enabled. Example: Server, Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the CSC Global CA APIs for Certificate Management:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

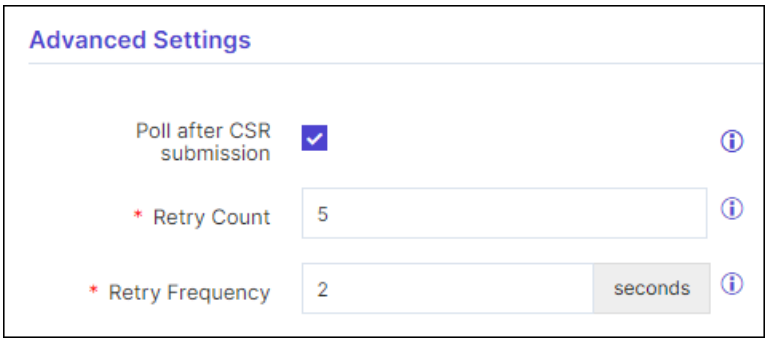


CA Configuration - Field Description Table

Fields	Description
***CA Base URL**	Enter the base URL that will be used to construct the API request. The value is *https://apis.cscglobal.com/dbs/api/v2*
***API Key**	Enter the API key which is a unique identifier used to authenticate the user. The value entered will be masked and encrypted.
Token	Enter the API token which is used to authenticate users or applications and provide access to protected resources. The value entered will be masked and encrypted.
*: *Mandatory fields*	

6. Click **Fetch Domain.**
   If the data provided is accurate the success message “Domains fetched successfully“ will be displayed and a table is displayed with two columns - *Account Number* and *Domain Name*. A list of active domains in AppViewX are listed in the table. Each account can hold multiple domains.
7. Update the following details in the **Advanced Settings** section as described in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Advanced Settings - Field Description Table

Fields	Description
***Poll after CSR submission**	Selecting the checkbox enables polling after CSR submission. It fetches the certificates immediately after CSR submission on enrollment, renew, and reissue with the retry count and retry frequency specified in the fields below.
***Retry Count**	Enter a value between 1 - 10.
***Retry Frequency**	Enter a value between 1 - 30 seconds.
*: *Mandatory fields*	

8. Click **Save**.
   - The CA details are saved in the CA instance inventory and the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

     Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

   - The **Fetch Custom Fields button** is enabled.

     Note: In case **Fetch Domains** and **Fetch Custom Fields** are not triggered before saving CA settings, this action can explicitly perform both these actions and update the CA.

9. To get the list of custom fields configured (if any), click **Fetch Custom Fields**.
   If the custom fields are configured they will be displayed in a table with two columns - *Name* and *Mandatory/Optional*.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Enter the values for the custom fields.
b. Click **Save**.

The details are saved.

Note: These custom fields attributes are displayed in the certificate enrollment form at the time of enrollment.

Validating CSC Global

Once the CSC Global CA settings are added, validation needs to be done to check whether the connection between AppViewX and CSC is properly configured.

1. On the CSC CA page, the above configured CA will be displayed with a **Check** button in the last column of the table.
2. Click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Custom CA

Prerequisites

The prerequisites for configuring Custom CA account in AppViewX are as follows:

- A logo to use it for the custom CA.
- An optional CA certificate and key to be used as a root certificate.

Configuring Custom CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Custom**.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Custom** home page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***Custom CA Name**	A unique name to identify the CA name. No special characters allowed.
***Upload Custom CA Logo**	Upload a logo for the custom CA. This logo will appear in the product representing the custom CA.
Custom CA Certificate	Upload a certificate for the custom CA. This certificate will become the root certificate. The <.*pfx*> and <.*p12*> are certificate types are supported.
*: *Mandatory fields*	

5. Once the logo and certificate are uploaded, the entered CA will appear in the CA list with the logo presented.
6. Once the logo is added, users can click **Configure Now** to input the CA details.
7. Update the following details in the **General Information** section as described in the table:

Fields	Description
***Name**	Client authentication certificate for API communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

8. Update the following details in the **ROOT CSR parameters** section as described in the table:

Root CSR - Field Description Table

Fields	Description
Common Name	The common name of the root certificate. • Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow users to request certificates with domain domain.com. • Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.)
Algorithm	Type of the root certificate.
Hash Function	The hash function for the root certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Organization Unit	Name of the Organisation unit.
Key Length	Key length for the root certificate.
Organization	Organization attribute for the root certificate.
Locality	Locality attribute for the root certificate.
State or Province	State attribute for the root certificate.
Country	Country attribute for the root certificate.
Email Address	Email address for the root certificate.
*: *Mandatory fields*	

9. Update the following details in the **Root Validity** section as described in the table.

Fields	Description
***Start Date**	Start date of the certificate issuance.
***End Date**	End date of the certificate issuance.
*: *Mandatory fields*	

10. Click **Save**.

    Once the setting is saved, the user will be directed to the root certificate submission holistic view as below.

11. Users can submit and fetch the root certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. On the CA setting page user can see the status of the created setting as shown below.

DigiCert CA

Important: Effective October 1st, 2025, DigiCert CA server certificates will include only server authentication in the Extended Key Usage (EKU). Dual authentication will no longer be supported.

As a temporary provision till May 01st, 2026, DigiCert CA will allow dual authentication in the EKU. Customers who need to continue enrolling server certificates with dual authentication enabled can contact AppViewX's Site Reliability Engineering (SRE) team for assistance at:

- saashelp@appviewx.com (for SaaS-based deployments)
- help@appviewx.com (for on-prem deployments)

However, it is strongly recommended to transition away from the use of server certificates for dual authentication to align with industry best practices.

Prerequisites

To configure a DigiCert CA account in AppViewX, you will need:

- A DigiCert CertCentral Account with one of the following roles:
  - **Administrator** (Full admin access including access to create divisions and users and to manage user access)
  - **Standard User** (Access to place and manage orders with changes being approved by a manager or administrator)
  - **Manager** (Access to mange finances, create and approve requests, manage orders and domains, and to view and edit users)
  - **Finance Manager** (Access to manage finances and to place and manage orders)
- API key

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Important: The API key is displayed only one time when it is generated. Ensure that it is copied and saved in a secure location.

- Account ID

For links to detailed instructions to get the above information from DigiCert, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring DigiCert

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the list of CAs displayed on the left, select **DigiCert**.
   The **DigiCert** CA account inventory is displayed. By default, the **DigiCert** CA tab is open.
3. If it is your first DigiCert CA integration in AppViewX, click **Configure Now**.
   The **Configure Now** button is displayed only if this is the first integration instance.

   For the subsequent integrations, from the top-right corner of the page, click **Add**.

   The **DigiCert** configuration page is displayed.
4. Enter/Select the **General Information** details for the DigiCert CA configuration.

General Information - Field Description Table

Fields	Description
***CA Account name**	Enter a unique name for the Certificate Account (CA) account, which will be displayed during certificate enrollment and policy creation. **Constraints**: • Valid special characters: **.**, **-**, and _ • CA account name should not begin with a special character and/or a space.
***Purpose/Usage**	From the dropdown list, select the certificate type(s) for which CLM actions will be enabled. **Possible values**: Server, Client, Code Signing
Proxy Required	For CA communication to happen via a proxy, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
Data Center (AppViewX's CA agent)	From the dropdown list, select the data center through which the CA communication must happen.
*: *Mandatory fields*	

5. To invoke the DigiCert CA APIs for certificate management, enter/select the **CA Configuration** details.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	Enter the base URL for constructing API requests. **Default value**: https://www.digicert.com/services/v2
***Credential Type**	From the following options in the dropdown list, select the method for providing authentication credentials for integrating DigiCert CA with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.
Account ID	Enter the account number provided for your DigiCert account.
***API Key**	The API key is a unique identifier that is used for authentication. In this field, enter the API key that has been generated for your DigiCert account.
***Credential List**	This field is displayed only when **Credential Type** = **Credential List - CyberArk**. The dropdown list is populated with credential entries stored in CyberArk. From the dropdown list, select the credential entry that will be used for authenticating the CA integration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Fetch Divisions and Certificate Types	To fetch the divisions and certificate types available in your DigiCert account, click **Fetch Divisions and Certificate Types**. AppViewX connects to DigiCert using the credentials provided to fetch the divisions (organizational units in DigiCert to manage certificates) and certificate types (available certificate types based on the **Purpose/Usage** selected).
Auto Approve	**Note:** This field has role-based access. It is disabled for the **Standard User** and **Financial Manager** roles. If all CLM requests from AppViewX do not need to be approved from the Digicert CA account, select the **Auto Approve** checkbox . Auto approval is optional and works only for **one-step certificate requests** configured in the Digicert Cert Central Account.
Discover additional fields	To fetch the custom attributes/additional certificate metadata configured for the DigiCert CA certificates, select this checkbox. These additional details are configured as vendor-specific details and custom certificate attributes at the time of certificate enrollment. **Important:** Enabling this field will have significant performance impact since an additional set of APIs must be executed to fetch the details.
*: *Mandatory fields*	

6. To fetch the custom attributes/additional certificate metadata details for this DigiCert CA integration, click **Fetch Custom Attributes**.

   Note: This field is displayed only when the **Discover additional fields** checkbox is selected.

7. Click **Save**.

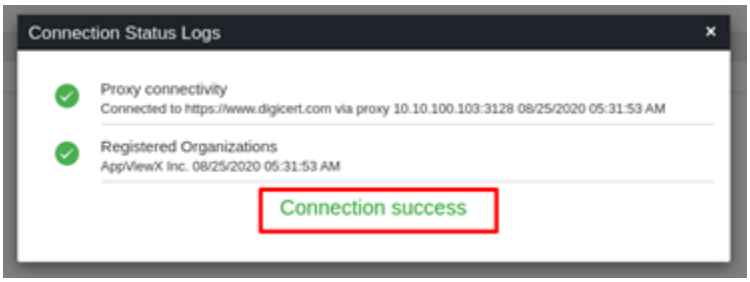
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the DigiCert CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Digicert**.
   The **Certificate Authority** page is updated to display an inventory of all DigiCert CA settings onboarded in AppViewX.
3. In the **Connection Status** column of the inventory grid, click **Check** to validate the CA setting.
   The CA communication will be validated and the **Connection Status** will be updated to**Success**/**Failure**.



References

Vendor documentation for retrieving DigiCert prerequisites:

- CertCentral (Centralized Certificate Management)
- Manage CertCentral Account
- Generate an API Key
- Set up your CertCentral Account

DigiCert MPKI

Prerequisites

The prerequisites for configuring a Digicert MPKI CA account in AppViewX are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- A Digicert MPKI Account with **Administrator** role Access.
- An **API Key** configured in Digicert MPKI with required permissions to make API Requests from AppViewX.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring DigiCert MPKI

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **DigiCert**.
   The **DigiCert** home page is displayed.
3. Click the **DigiCert MPKI** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **DigiCert MPKI** configuration page is displayed.
5. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

6. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Digicert CA APIs for Certificate Management.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Configuration - Field Description Table

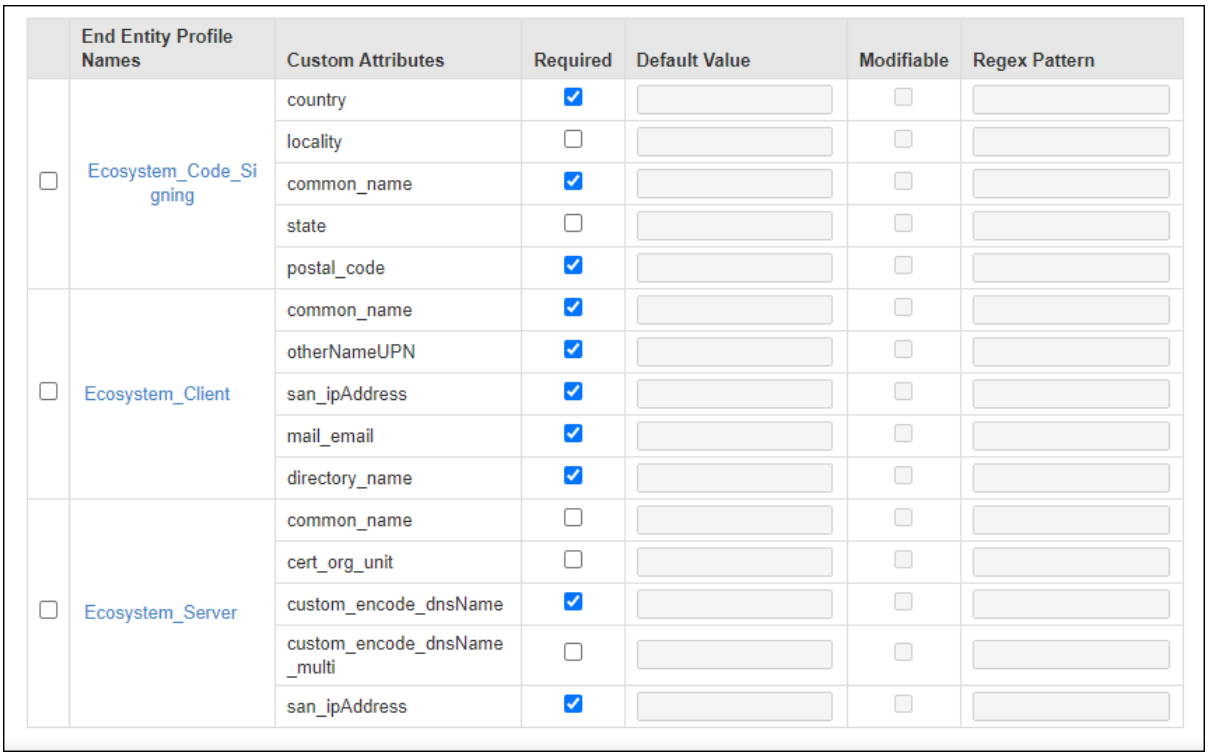
Fields	Description
***Base URL**	This URL will contain just the hostname of the Digicert CA instance. For example, <https://www.digicert.com>
***Seat ID**	Enter the unique seat id for discovering certificates.
***API Key**	Enter the API key, which is generic across all CAs

*: *Mandatory fields*

Note: Auto approval checkbox is optional and features work only for **one-step certificate requests** configured in the DigiCert Central Account.

7. Select **Fetch Divisions and Certificate Types.**

   The Division and Certificate types available in the Digicert CA account will be fetched and listed for the specific API key user in the table as shown below.



	End Entity Profile Names	Custom Attributes	Required	Default Value	Modifiable	Regex Pattern
☐	Ecosystem_Code_Signing	country	☑		☐	
		locality	☐		☐	
		common_name	☑		☐	
		state	☐		☐	
		postal_code	☑		☐	
☐	Ecosystem_Client	common_name	☑		☐	
		otherNameUPN	☑		☐	
		san_ipAddress	☑		☐	
		mail_email	☑		☐	
		directory_name	☑		☐	
☐	Ecosystem_Server	common_name	☐		☐	
		cert_org_unit	☐		☐	
		custom_encode_dnsName	☑		☐	
		custom_encode_dnsName_multi	☐		☐	
		san_ipAddress	☑		☐	

8. Click **Save**.

   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully

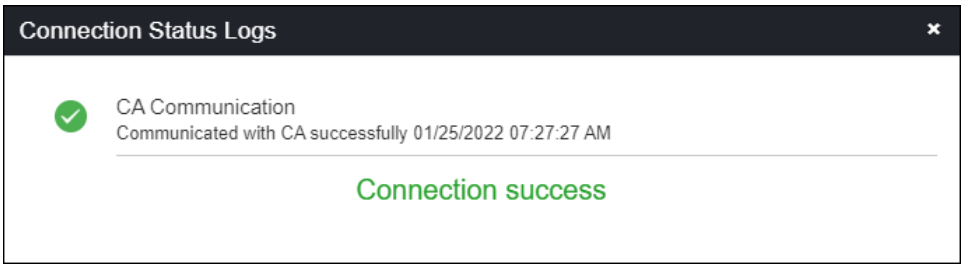
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the DigiCert MPKI Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **DigiCert**.
   The **DigiCert** home page is displayed.
3. Click **DigiCert MPKI** from the left pane of the page.
   The **DigiCert MPKI** home page is displayed.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



DigiCert One

Prerequisites

In order to configure a DigiCert One CA account you will need the following:

- DigiCert One account base URL
- API Key or Client Authentication certificate (depending on the authentication mode)

For links to detailed instructions to get the above information from DigiCert One, see the **References** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a DigiCert One CA Account

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
   The **Certificate Authority** page is displayed.
2. On the **Certificate Authority** page, from the CA list displayed in the left, select **DigiCert**.
   The **Certificate Authority** page for **DigiCert** is displayed.
3. Click the **DigiCert One** tab.
4. To onboard your first DigiCert One CA account setting in AppViewX, click **Configure Now**.
   OR

   Click **+Add**.

   The **Certificate Authority** page is updated to display the form fields for onboarding a DigiCert One CA account.
5. Enter/Select the **General Information** for the CA account.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	From the dropdown list, select the certificate type for which the CLM actions have to be enabled.
Proxy Required	Enable this field if the CA communication needs to happen via a proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

6. Enter/Select the **CA Configuration** details.

General Information - Field Description Table

Fields	Description
***Base URL**	Hostname of DigiCert One instance. For example http://one.digicert.com

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Authentication method**	From the following options, select an authentication method for authenticating the API requests: • **API Token**: To authenticate the API requests with an API token, select this option. • **Client Certificate**: To authenticate the API requests using a client certificate file, select this option. **Important:** Currently, only the **API Token** authentication method is supported.
***API Key**	Enter the API key that will be used for authentication. **Note:** You will be assigned an API key when you login to your DigiCert One instance and create a user.
Allow Seat ID during enrollment	Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. For the certificates enrolled for this CA account, you can either assign a unique seat ID for each certificate or a common one for all the certificates. To assign a unique Seat ID for the certificates enrolled for this CA account, select this checkbox. If you select this option, a field to specify the seat ID is hidden from the CA settings form and is included in the certificate enrollment form.
***Seat ID**	Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. To have a common Seat ID for all certificates enrolled for this CA account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Use DigiCert One to switch certificates from DigiCert MPKI	To automatically switch your DigiCert MPKI certificates to DigiCert One at the time of auto regeneration, select this checkbox. **Important:** For multiple CA accounts with automatic CA switch enabled, CA switch will use CA settings configured for the first CA account for which the automatic CA switch is enabled. **Note:** To manually switch CAs, refer to the instructions here.
*: *Mandatory fields*	

7. To fetch profiles that are assigned to the configured user which will be used during certificate enrollment, policy creation, through out the product, click **Fetch Certificate Profiles**.
   All certificate profile configured with “enrollment_method”: **rest_api** and “authentication_method”: **third_party_app** are displayed.
8. Click **Save.**
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

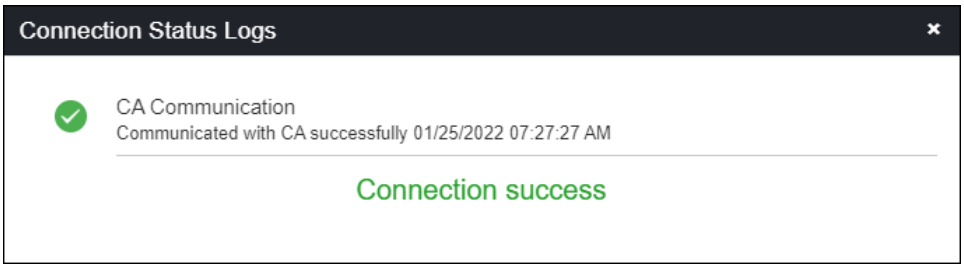
Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the DigiCert One CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
   The **Certificate Authority** page is displayed.
2. On the **Certificate Authority** page, from the CA list displayed in the left, select **DigiCert**.
   The **Certificate Authority** page for **DigiCert** is displayed.
3. Click the **DigiCert One** tab.
   All existing DigiCert CA accounts are listed in the inventory on this page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the **Connection Status** column, click **Check**.
   The CA communication is validated and a success/failure message is displayed.



References

Vendor documentation for retrieving DigiCert One prerequisites:

- Retrieving the base URL
- Creating your API token
- Creating your API token authentication certificate

EJBCA

Prerequisites

A client certificate and URL are needed to configure the EJBCA account in AppViewX.

- The URL must be entered in the format **https://<node_hostname>:<port>/ejbca/ejbcaws/ejbcaws?wsdl**. The **node hostname** is available on the UI of the EJBCA adminweb portal's welcome screen.
- An EJBCA client certificate for a user having the necessary access for enrolling the certificates and other CLM operations. To issue a client authentication certificate in EJBCA, do the following:
  1. In EJBCA, click RA Web to access the EJBCA RA user interface.
  2. To enroll, select **Enroll** > **Use Username** and specify the following:
     - **Username:** Enter the username as specified earlier in the step Add end entity
     - **Enrollment code:** Enter the password specified earlier in the step Add end entity.
     - Click **Check**.
     - For Key algorithm, you can limit the type of keys to be used, such as only RSA 2048 bits.
     - Click **Download PKCS#12** to download and save the keystore.
- AppViewX server (worker node) / CC should either have internet access/EJBCA endpoint URL access, have a proxy configured in general settings (if required). Refer to the section Managing Proxy Settings in the Platform guides.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **For SaaS**: 443 communication from the preferred CC (Cloud Connector) to EJBCA API / endpoint URL.
- **For On-Prem**: Workers nodes should have internet access or the proxy should be configured in General Settings for connectivity to EJBCA API / endpoint URL.

Configuring EJBCA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **EJBCA**.
   The **EJBCA** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **EJBCA** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/ Usage**	Certificate Type for which CLM actions will be enabled. E.g. Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the APIs for Certificate Management.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Configuration - Field Description Table

Fields	Description
***Client Authentication**	Client authentication certificate for API communication. a. Enter the valid password once the **Authentication Details** window is displayed. b. Click **OK**. The value must be a valid <.*p12*> or <.*pfx*> file.
***URL**	EJBCA URL in the format *https://<node_hostname>:<port>/ejbca/adminweb/*
Click **Validate and Fetch**. The **End entity profiles** available for the CA account will be fetched along with the certificate profile from the **Certificate Authority**.	
***Communication mode**	Choose any of the following modes; it is required for CA Discovery. • **SOAP** • **REST**
***Discover by expiry days**	Set the number of days to expiry, which is calculated from the current day. The value must be number.
*: *Mandatory fields*	

6. Update the following details in the **Certificate Attributes** section as described in the table:

Fields	Description
***End Entry Profile Names**	Select the profile that is used in the certificate enrollment from the dropdown list. This is the required end entity profiles for CA setting.
Custom Attributes	Select the list attributes configured in CA to enroll certificates. These are the required custom attributes for the specific end entity profile. Custom attributes should be configured as exactly as it is available in the EJBCA portal. (Validation can be added by the user in the regex box, check if mandatory and modifiable).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

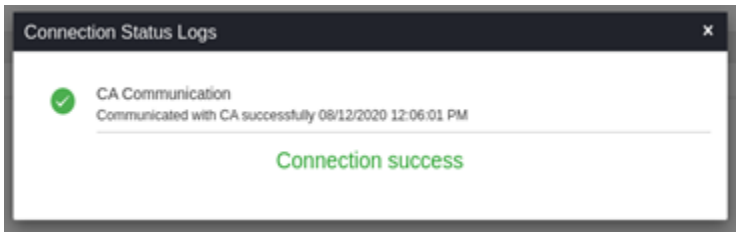
Fields	Description
*: *Mandatory fields*	

7. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the EJBCA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **EJBCA**.
   The **EJBCA** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



Entrust CA

Prerequisites

To configure a Entrust CA account in AppViewX, you will need:

- An Entrust client authentication certificate
- Credentials (API username and API key) for an account with the requisite access for executing CLM actions

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For links to detailed instructions to get the above information from Entrust, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring Entrust

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed. The Entrust tab is selected by default.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Entrust** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example: Server and Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Entrust CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Client Authentication**	The client authentication certificate from Entrust for API communication.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Must be a valid <.*p12*> file. To generate an CSR within AppViewX refer to Generating a CSR and download the CSR. Further, upload the CSR to the Entrust homepage.
***Base URL**	This URL will contain just the hostname of the Entrust CA instance. The default value is *https://api.entrust.net/enterprise/v2*.
***API Username**	Enter the API Username to communicate with the CA.
***API Key**	Enter the API Password to communicate with the CA.
Auto Approve	Select the checkbox to avoid queuing of new certificates in the CA portal.
**: Mandatory fields*	

6. Update the following details in the **Advanced Settings** section as described in the table.

Advanced Settings - Field Description Table

Fields	Description
Poll after CSR Submission	A check box field when selected will fetch the certificated immediately after CSR Submission on enrollment, renew, and reissue of certificate with the retry count and retry frequency as described below.
***Retry Count**	The number of times the polling will take place after CSR submission. Enter a value between 1 and 10.
***Retry Frequency**	The duration of the polling. enter the value between 1 and 30seconds
**: Mandatory fields*	

7. Click **Fetch Custom Attributes**.
   The attributes available for the CA account will be fetched from the Certificate Authority along with the CA and profile names. A pop-up message is displayed as **CA and profiles fetched**.
8. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully

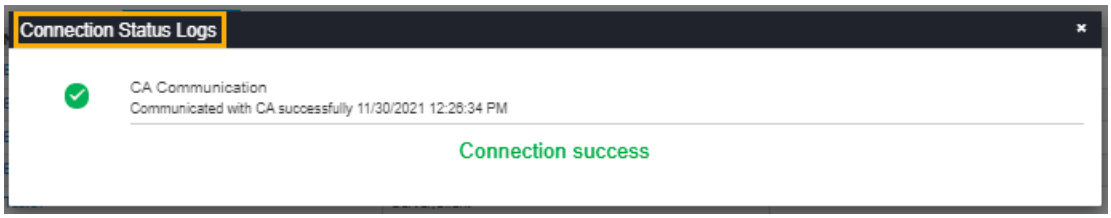
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Entrust CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



References

Vendor documentation for retrieving Entrust prerequisites:

- Entrust REST PKI Guide

  Downlad the Entrust REST PKI Guide and refer to the section **Authentication** > **TLS with client certificate authentication**.

Entrust MPKI

Prerequisites

To configure a Entrust MPKI account in AppViewX, you will need:

- Base URL
- Client authentication certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For links to detailed instructions to get the above information from Entrust MPKI, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring Entrust MPKI

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed.
3. Click the **Entrust MPKI** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Entrust MPKI** configuration page is displayed.
5. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example: Server and Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Entrust MPKI CA APIs for Certificate Management.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Configuration - Field Description Table

Fields	Description
***Client Certificate**	Client authentication certificate for API communication. Click the **Upload** button to select and upload the client certificate. **Note:** Must be a valid <*.p12*> file. You will be prompted to enter a **Password** for the certificate.
***Base URL**	This URL will contain just the hostname of the Entrust CA instance. Eg - https://api.entrust.net/enterprise/v2
**: Mandatory fields*	

7. Click **Fetch CA and Profile Names.**
   The attributes available for the CA account will be fetched from the Certificate Authority along with the CA and profile names. A pop-up message is displayed as **CA and profiles fetched**.
8. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

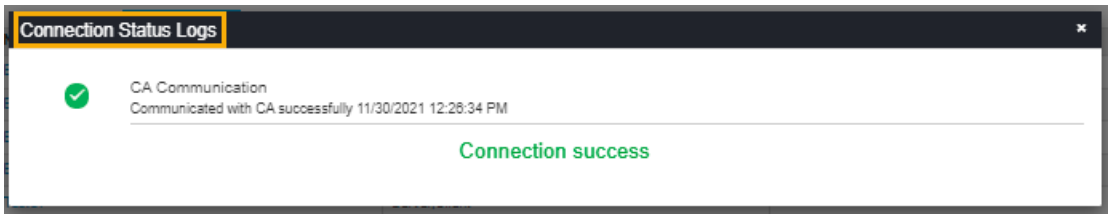
Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Entrust MPKI Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Entrust**.
   The **Entrust** home page is displayed.
3. Click **Entrust MPKI** from the left pane of the page.
   The **Entrust MPKI** home page is displayed.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



References

Vendor documentation for retrieving Entrust MPKI prerequisites

Please contact the Entrust MPKI team for assistance.

Futurex

Important: For the AppViewX-Futurex integration, the current implementation supports only the certificate enrollment, regeneration, and auto-regeneration CLM actions. Support for the certificate renewal, auto-renewal, and revocation CLM actions will be included in the subsequent releases.

Prerequisites

To onboard a Futurex CA setting in AppViewX, you will need:

- KMES Host API URL and port number
- Login credentials

  For links to detailed instructions on getting the above information from Futurex, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring a Futurex CA Account in AppViewX

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
   The **Certificate Authority** page is displayed.
2. On the **Certificate Authority** page, from the CA list displayed in the left, select **Futurex**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If this is the first Futurex CA setting to be onboarded in AppViewX, the **Certificate Authority** page is updated to display the **Configure Now** button for Futurex.

If this is a subsequent CA setting, the **Certificate Authority** is updated to display an inventory of the existing Futurex CA settings.

3. To onboard your first Futurex account setting in AppViewX, click **Configure Now**.
   OR

   Click **+Add**.

   The **Certificate Authority** page is updated to display the form fields for onboarding a Futurex account.
4. Enter/Select the **General Information** for the CA account.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. Names should not start with special characters. **Constraints**: • Only the following special characters are considered valid: **.**, **-**, and _. • The CA account name cannot start with a special character (including the valid ones).
***Purpose/Usage**	From the dropdown list, select the certificate type (server, client, and code signing) for which the CLM actions have to be enabled.
Proxy Required	If the CA communication has to happen via a proxy, select this checkbox. Proxy settings configured in the **Platform** module of the product will be used for the communication. To read more on how the proxy is set up, click here.
Data Center (AppViewX's CA agent)	From the dropdown list, select the data center through which the CA communication will be routed.
*: *Mandatory fields*	

5. Enter/Select the **CA Configuration** details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***API Endpoint**	Enter the endpoint URL of the KMES remote host, without the port number. **Constraints**: • **Valid input values** • Letters (a–z, A–Z) • Numbers (0–9) • Hyphen (-) • Period (.) • Forward slash (/) • Colon (:) • Protocol prefix (`http://` or `https://`) • **Invalid input values** • Port numbers (for example, 443) • Backslash (\) • Single and double quotation marks (', '') • Angle brackets (<, >) • Braces ({, }) • Caret (^) • Pipe (|) • Backtick (`)
***Port**	Enter the KMES host API port number. **Constraints**: • Only numeric values are allowed. • Input value must be in the range **1** - **65535**.
***Authentication method**	From the dropdown list, select the authentication method that will be used for connecting to the KMES host API. Currently, for onboarding a Futurex CA setting, AppViewX supports authentication only via **Username and Password**. The corresponding value in the dropdown list is selected, by default.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Number of logins required**	Futurex issues multiple login credential sets to each account. For stronger security, users can be asked to login with more than one credential set. To set how many credentials a user must provide for authentication, enter the required number in this field. **Valid values**: **1** to **9**
***User Name**	Enter the username for connecting to Futurex KMES host API.
***Password**	Enter the password for connecting to Futurex KMES host API.
Add	To add the above configured CA setting to the FutureX CA settings inventory in AppViewX, click **Add**.
Client Certificate required	[Optional] To use a client certificate to communicate with the host API endpoint, turn on the **Client Certificate required** toggle. This will require users to provide a valid PKCS12 client certificate, in the **.p12** or **.pfx** format, for authentication before they are connected to the Futurex KMES host API.
Client Authentication Certificate	This field is displayed when the **Client Certificate required** security feature is enabled. **Note:** Only **.p12** and **.pfx** PKCS12 client certificates can be uploaded for authentication. To upload a client certificate for authentication: a. Click **Upload**. b. Navigate to the location of the client certificate file and select the required certificate file.
*: *Mandatory fields*	

6. To retrieve the complete list of issuance policies supported by this Futurex CA setting, click **Fetch Issuance Policies**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

An issuance policy defines the rules, restrictions, and configuration for how a Certificate Authority (CA) issues certificates. It controls the approval requirements, cryptographic settings, alerts, and other configuration parameters.

The retrieved list is displayed in a table below the **Fetch Issuance Policies** button.

7. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done manually.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
   The **Certificate Authority** page is displayed.
2. On the **Certificate Authority** page, from the CA list displayed in the left, select **Futurex**.
   The **Certificate Authority** page is updated to display an inventory of all Futurex settings onboarded in AppViewX.
3. In the **Connection Status** column of the inventory grid, click **Check** to validate the CA setting.
   The CA communication will be validated and the **Connection Status** will be updated to**Success**/**Failure**.

References

- Futurex Documentation

GlobalSign MSSL CA

Prerequisites

To configure a GlobalSign MSSL CA account in AppViewX, you will need:

- SSL URL
- GlobalSign administrator account
- Manager and Staff in charge user roles

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For links to detailed instructions to get the above information from GlobalSign MSSL, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring GlobalSign MSSL

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click the **GlobalSign MSSL** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GlobalSign MSSL** configuration page is displayed.
5. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, server and clients
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Update the following details in the **CA Configuration** section as described in the table.

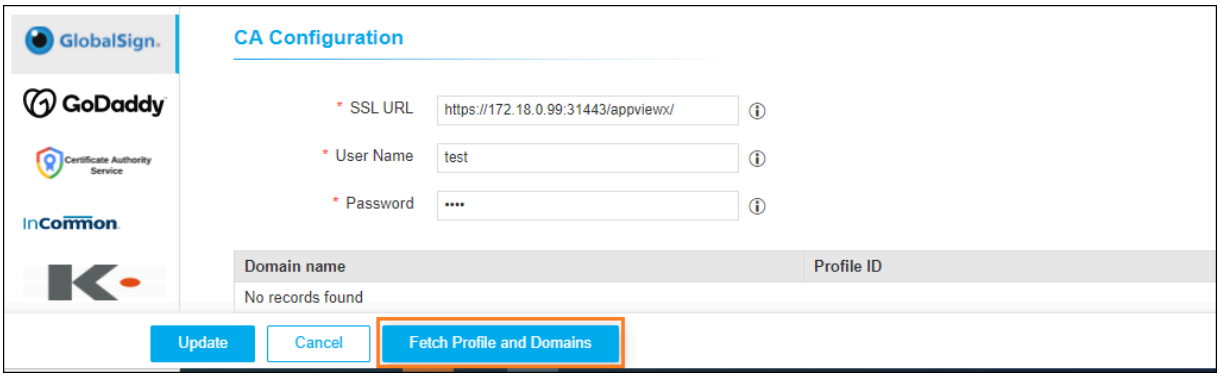
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***SSL URL**	Base URL of the SSL API
***User Name**	Provide a username of the GCC to communicate with the CA.
***Password**	Provide a password for the GCC to communicate with the CA.
**: Mandatory fields*	

7. Once all the details are configured, click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

8. In GlobalSign MSSL, we can now fetch profiles and domains by clicking on the **Fetch Profiles and Domain** button.

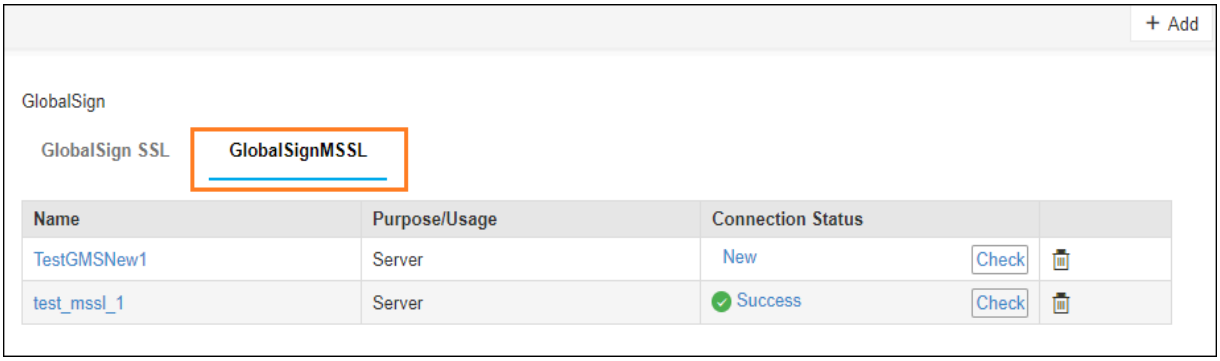


> **Note:** The supported CSR key types are RSA **2048-8192, ECC P-256, ECC P-384** .

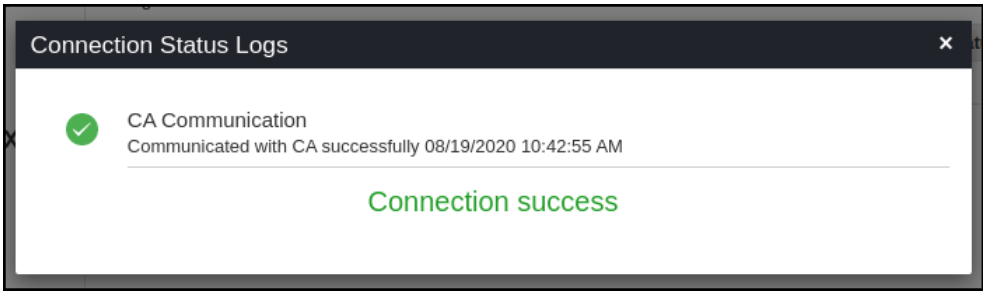
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Manually Validating the GlobalSign MSSL Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **GlobalSign MSSL** from the left pane of the page.
   The **GlobalSign MSSL** home page is displayed.



4. In the **Status** column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**



Limitations

Once the GlobalSign MSSL settings are added, validation needs to be done to check whether the connection between AppViewX and GlobalSign MSSL is properly configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Case/ Ticket number	Fix Description
CA Setting Update	Users need to click on the **Cancel** button once the MSSL domain/profile. ID details are fetched from the GlobalSign MSSL account. If the user clicks the Update button, MSSL domain/profile ID details will be removed from the associated policy. The steps to follow to update CA settings are as follows: 1. On the GlobalSign MSSL CA settings page, after adding/editing values, click the Update button. 2. Navigate back to updated CA settings and click the **Fetch Profiles and Domain** button. 3. Click the **Cancel** button instead of Update to bypass the existing issue.
Default CA policy mapping	The default CA policy is defined with all available values selected and validity data is mapped based on commonly used validity. Hence, it will not have values equivalent to API documents or CA portals. This can be modified or updated in the application accordingly to the default CA policy if changes are required.
Email Address	The email address provided in the email address field on the enrollment page is not considered as the primary email value during CLM actions, instead, the email address field defined in the contact information of the logged-in user will be used. The help info message besides the Email address field on enroll/edit page is as – “If the user email address is configured, that will be used for GlobalSign CA approval actions. If the user email is not configured, then the email address provided in this field will be used" - the second part is not valid anymore.

References

Vendor documentation for retrieving GlobalSign MSSL prerequisites:

- GlobalSign API Guide for MSSL Certificates

  Download the PDF and refer the section **API and WSDL URLs**.

- Contact the GlobalSign MSSL CA team for setting up the initial administrator account to be able to create user roles.
- Create new user accounts.

GlobalSign Atlas CA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

To configure a GlobalSign Atlas CA account in AppViewX, you will need:

- Base URL
- API key and secret key
- Client certificate

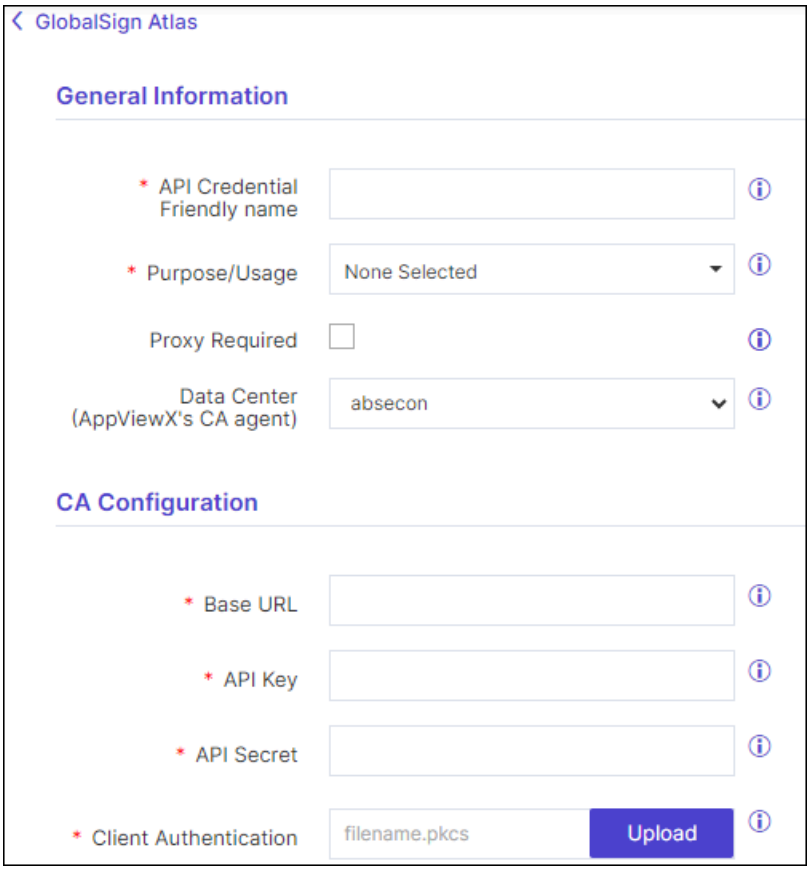
  For links to detailed instructions to get the above information from GlobalSign Atlas, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring GlobalSign Atlas

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Choose the **GlobalSign Atlas** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GlobalSign Atlas** configuration page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***API Credential Friendly name**	Enter the API Credentials Friendly name (which is the CA Account name that will be used for the CA Policy and Enrollment).
***Purpose/Usage**	Select the purpose of the certificate that can be requested using this account. **Note:** Users can select *Server*, *Client* or both.
Proxy Required	Select the checkbox if communication to the Certificate Authority (CA) has to use the proxy details provided in the general settings
Data Center (AppViewX's CA agent)	Select the data center that will be used to establish the communication with the CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. Update the following details in the **CA Configuration** section as described in the table.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	Enter the base URL required for constructing the API request.
***API Key**	Enter the API key which is the unique identifier used to authenticate a user. **Note:** The API Key will be displayed as asterisks (*)
***API Secret**	Enter the API secret to communicate with the CA. **Note:** The API Key will be displayed as asterisks (*)
***Client Authentication**	Upload the certificate for client authentication in the .p12 or .pfx format only.
*: Mandatory fields	

7. Click the **Fetch Validation Policy and Save** button.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

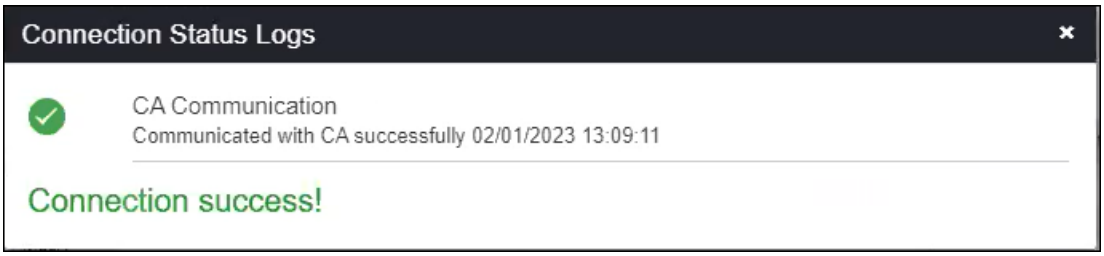
Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the GlobalSign Atlas Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click **GlobalSign Atlas** from the left pane of the page.
   The **GlobalSign Atlas** home page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **Status** column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



References

Vendor documentation for retrieving GlobalSign Atlas prerequisites:

- GlobalSign Atlas Certificate Management API Guide

  Download the PDF and refer the **Overview** section.
- Generate API credentials.
- Order a new client certificate.

GlobalSign SSL CA

Prerequisites

To configure a GlobalSign SSL CA account in AppViewX, you will need:

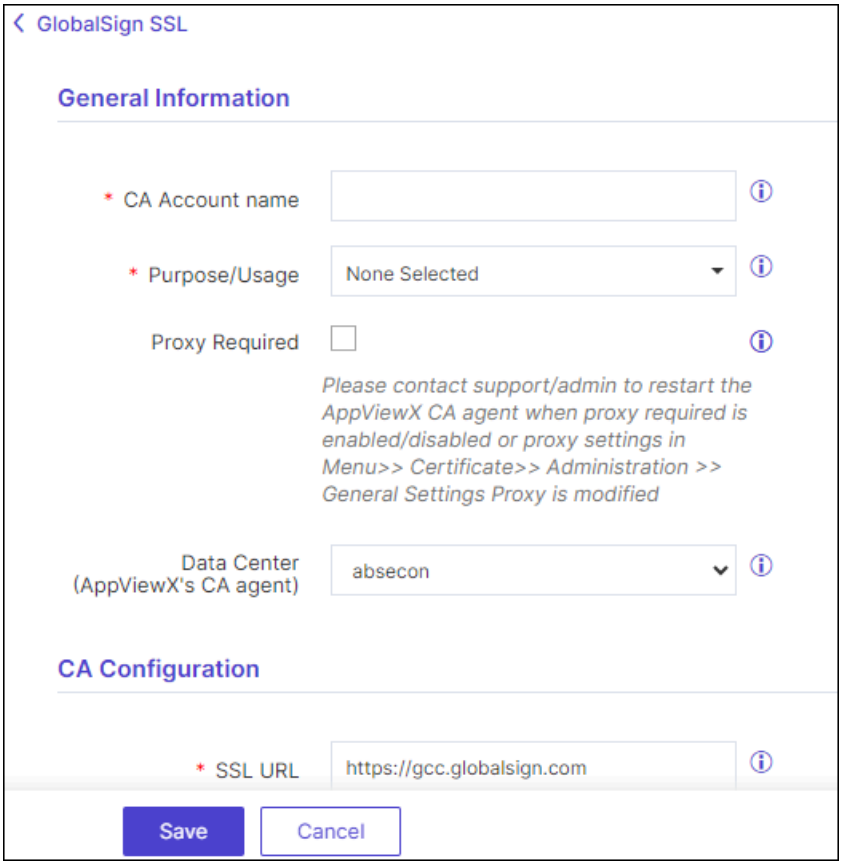
- SSL URL
- GlobalSign administrator account
- Manager and Staff in charge user roles

  For links to detailed instructions to get the above information from GlobalSign SSL, see the **References** section.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring GlobalSign SSL

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click the **GlobalSign SSL** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GlobalSign SSL** configuration page is displayed.



5. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server and Client.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Update the following details in the **CA Configuration** section as described in the table.

CA Configuration - Field Description Table

Fields	Description
***SSL URL**	Base URL of the SSL API.
***User Name**	Provide a username of the GCC to communicate with the CA.
***Password**	Provide a password for the GCC to communicate with the CA.
**: Mandatory fields*	

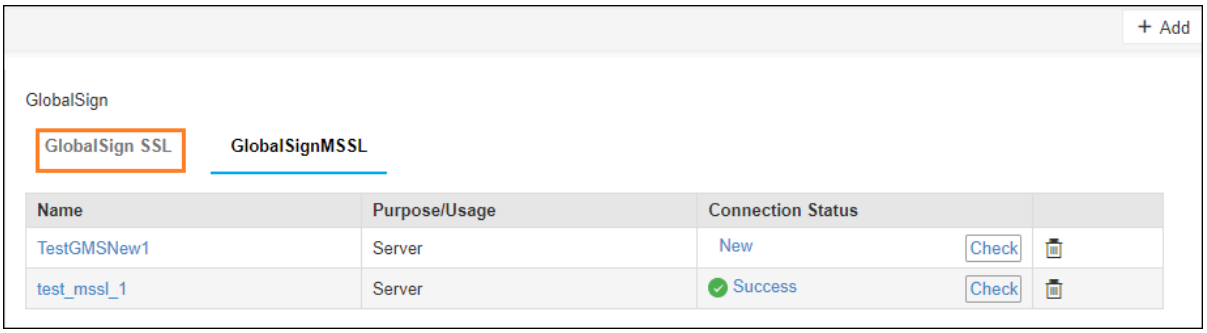
7. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

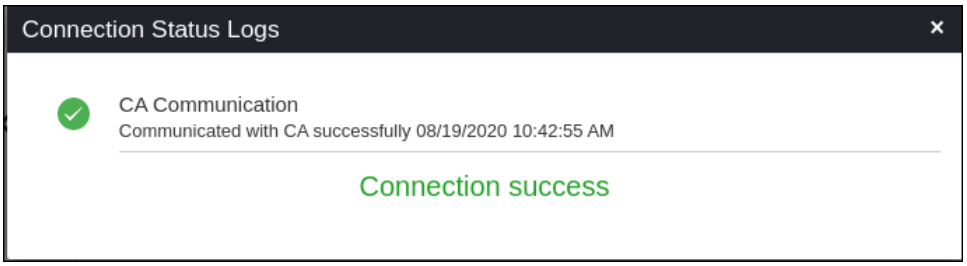
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Manually Validating the GlobalSign SSL Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GlobalSign**.
   The **GlobalSign** home page is displayed.
3. Click **GlobalSign SSL** from the left pane of the page.
   The **GlobalSign SSL** home page is displayed.



4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the Connection Status will be shown as either Success or Failure.



References

Vendor documentation for retrieving GlobalSign SSL prerequisites:

- GlobalSign API Guide for SSL Certificates

  Download the PDF and refer the section **WSDL and API URLs**.

- Contact the GlobalSign MSSL CA team for setting up the initial administrator account to be able to create user roles.
- Create new user accounts.

GoDaddy CA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

To configure a GoDaddy CA account in AppViewX, you will need:

- GoDaddy Customer Number, API key, and secret for making API Requests from AppViewX in order to perform CLM (Certificate Lifecycle Management) operations

  For links to detailed instructions to get the above information from GoDaddy, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.
- Product units in your GoDaddy account to perform CLM operations

Configuring GoDaddy

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GoDaddy**.
   The **GoDaddy** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **GoDaddy** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the GoDaddy CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain the Base URL of the GoDaddy CA API instance. For example: https://api.godaddy.com
***Customer Number**	Each user will have a unique customer number which is used to obtain the certificates from the GoDaddy CA account.
***API Key**	API key generated in the GoDaddy portal which is used for GoDaddy API communications.
***API Secret**	API Secret generated in the GoDaddy portal which is used for GoDaddy API communications.
First Name	First name of the GoDaddy Account user's name as provided in the portal to be used for certificate creation purposes.
Last Name	Last name of the GoDaddy Account user's name as provided in the portal to be used for certificate creation purposes.
Email Address	Email Id of the GoDaddy Account user's name as provided in the portal to be used for certificate creation purposes. **Note**: Valid email address.
Phone Number	Phone number of the GoDaddy Account user as provided in the portal to be used for certificate creation purposes. **Note:** Phone numbers must contain a minimum of 7 and a maximum of 15 numeric values.
**: Mandatory fields*	

6. Click **Save**.

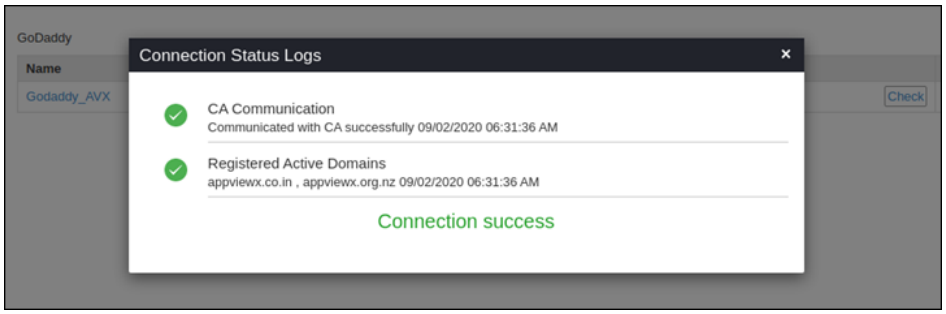
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the GoDaddy CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GoDaddy**.
   The **GoDaddy** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



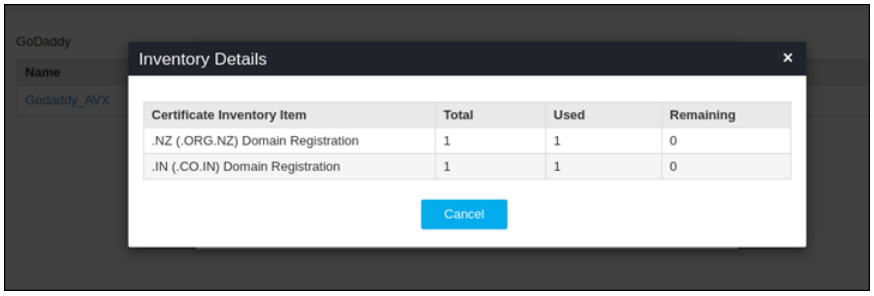
Viewing GoDaddy Product Units

Each GoDaddy account has different types of SSL products and units. The below steps will allow users to know the availability of the products and their remaining units.

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **GoDaddy**.
   The **GoDaddy** home page is displayed.
3. On the **GoDaddy** page, click **View** to fetch the product types and the units available for the GoDaddy account configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Once clicked, users can view the available and used product units.



References

Vendor documentation for retrieving GoDaddy prerequisites:

- Get Started with GoDaddy Setup

Google CA

Prerequisites

The prerequisites for configuring a Google CA account in AppViewX are as follows:

- Ensure all necessary setup is completed on the Google CA portal.

  For references, click here.
- A Google client certificate or Google client authentication Json for a user having necessary access for enrolling the certificates and for other Certificate Lifecycle Management (CLM) operations.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Refer to the section Managing Proxy Settings in the Platform guides.
- The URL https://www.googleapis.com should be reachable from AppViewX.

Configuring Google

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Google**.
   The **Google** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Google** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server and Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Configure either Certificate Upload or JSON Upload. These fields are necessary for invoking the Google CA APIs via Certificate Upload for Certificate Management. Select the Certificate Upload check box,
   Update the following details in the **CA Configuration** section as described in the table.

Fields	Description
***Certificate and Key**	Client authentication certificate for API communication.
***Email address**	Email address of the user
***Project Id**	Id of the project
**: Mandatory fields*	

6. Select the JSON Upload check box and configure a CA. Click the Upload button to upload the JSON file.
7. Click **Validate and Fetch**. The issuer names available for the CA account will be fetched along with the validity of the issuers from the Certificate Authority.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

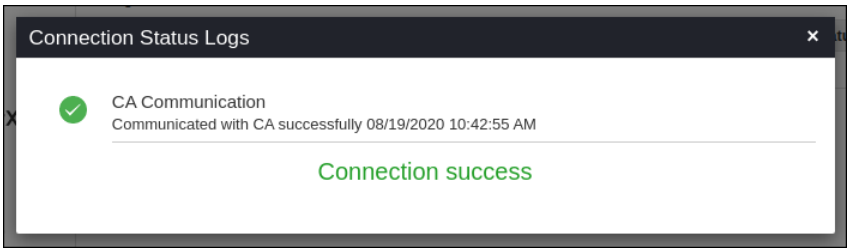
Location	CA Name	Validity	Delete
us-central1	pre-prod-root-ca	05/13/2030 20:02:21	
	testbed-root-ca	05/13/2030 20:27:49	
	prod-root-ca	04/23/2030 12:23:32	
	prod-inter-ca-level-981	06/14/2020 09:03:33	
	prod-inter-ca-level-200	06/14/2020 09:08:43	
	prod-inter-ca-level-201	06/14/2020 09:09:09	
	prod-inter-ca-level-000	06/14/2020 08:51:09	
	prod-inter-ca	04/23/2030 12:27:40	
	prod-inter-ca-level-01	06/14/2020 09:00:50	
europe-west1	test-bed-root-ca	05/13/2030 21:09:13	

8. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Google CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **Google**.
   The **Google** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   CA communication will be validated and the Connection Status will be shown as either Success or Failure.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Vendor documentation for Google CAS permissions:

- Permissions list
- Key creation and exporting as JSON or p12

HashiCorp Vault CA

Prerequisites

To configure a HashiCorp Vault CA account in AppViewX, you will need:

- Login and password to access AppViewX
- Base URL, role ID, and secret key for the **AppRole** method
- Base URL, access key, secret key, and role name for the **AWS** method

  Please contact the HashiCorp Vault team for retrieving the above listed prerequisite values.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring HashiCorp Vault

Steps to Configure HashiCorp Vault CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **HashiCorp Vault**.
   The **HashiCorp Vault** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **HashiCorp Vault** configuration page is displayed.
4. Update the details in the General Information section as described in the table below:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-', and '_' are allowed. Names should not start with special characters.
***Purpose/Usage**	The dropdown contains checkboxes for the certificate type for which the CLM actions will be enabled. The values are: • Server • Client • Code Signing One or more values can be selected depending on the type of account users need to create.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the details in the **CA Configuration** section as described in the tables below. These fields are necessary for invoking the Hashicorp CA Secret Engine for Certificate Management. The fields displayed in the CA Configuration section depend on the value selected in the **Method** field. The two auth method values are
   - **APP ROLE** - The APP ROLE auth method allows machines or apps to authenticate with Vault-defined roles. An "AppRole" represents a set of Vault policies and login constraints that must be met to receive a token with those policies. An AppRole can be created for a particular machine, or even a particular user on that machine or a service spread across machines. The credentials required for successful login depend upon the constraints set on the AppRole associated with the credentials.
   - **AWS** - The AWS auth method provides an automated mechanism to retrieve a Vault token for IAM principals and AWS EC2 instances. Unlike most Vault auth methods, this method does not require manual first-deploying or provisioning of security-sensitive credentials (tokens, username/password, client certificates, etc), by operators under many circumstances.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Configuration for App Role - Field Description Table

Fields	Description
***Base URL**	The base of URL of the CA account.
***Method**	**APP ROLE**
***Role ID**	RoleID is an identifier that selects the AppRole against which the other credentials are evaluated. When authenticating against this auth method's login endpoint, the RoleID is a required argument at all times. By default, RoleIDs are unique UUIDs, which allow them to serve as secondary secrets to the other credential information.
***Secret Key**	Secrey Key (SecretID) is a credential that is required by default for any login and is intended to always be secret. They can be created against an AppRole either via generation of a 128-bit purely random UUID by the role itself or via specific, custom values. Similarly to tokens, Secret keys have properties like usage-limit, TTLs and expirations.
**: Mandatory fields*	

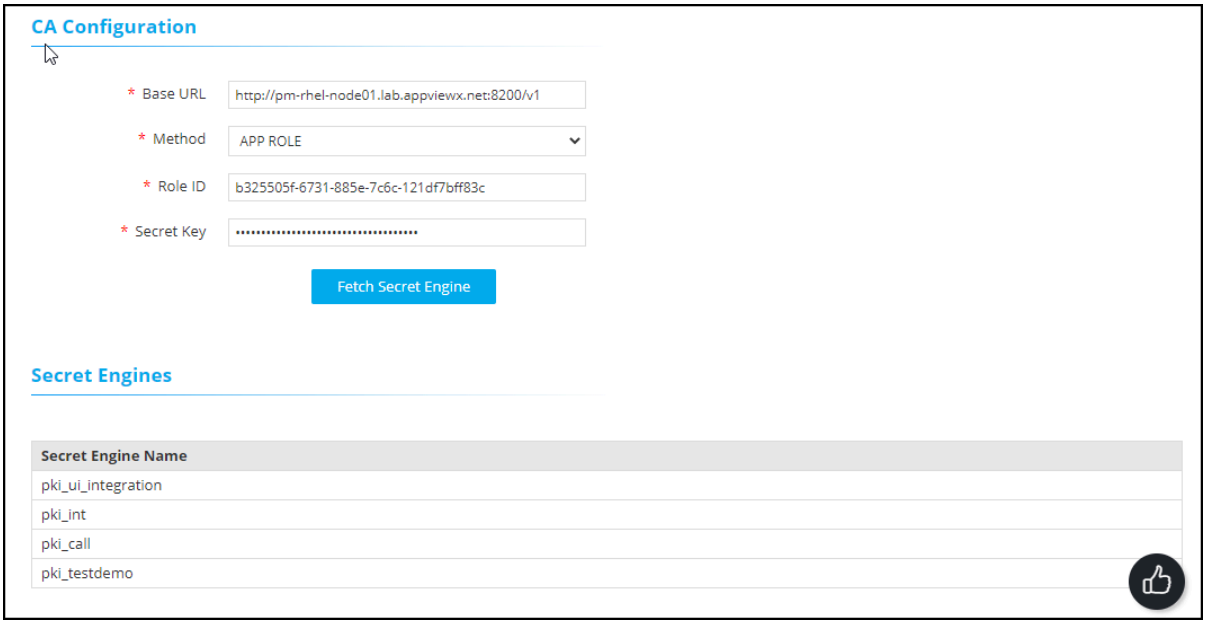
CA Configuration for AWS - Field Description Table

Fields	Description
***Base URL**	The base of URL of the CA account.
***Method**	**AWS**
***Access Key**	Access Keys are used to sign the requests that are sent. Access Key and Secret Key are used for programmatic (API) access to AWS services.
***Secret Key**	Secret Key (SecretID) is a credential that is required by default for any login and is intended to always be secret. Similar to tokens, SecretIDs have properties like usage-limit, TTLs, and expirations.
***Role Name**	The basic mechanism of operation (AWS authorization workflow) is per-role. Roles are registered in the method and associated with a specific authentication type that cannot be changed once the role has been created. Roles can also be associated with various optional restrictions, such as the set of allowed policies and max TTLs on the generated tokens.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The correct values entered in the fields establish a connection with the Hashicorp vault to be able to fetch the secret engine.

6. Click the **Fetch Secret Engine** button.
   A list of PKI secret engines is displayed. These will be presented to users in the policy. from where they can select the respective secret engines.



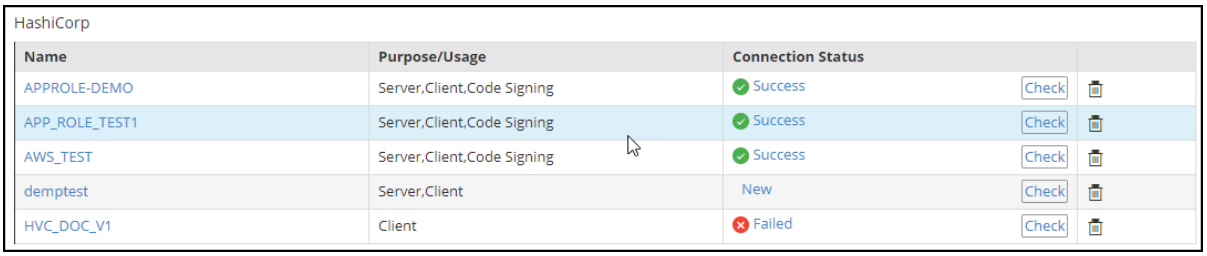
7. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Editing an Account

1. Go to the **HashiCorp Vault** CA account home page
   The list of Accounts is displayed in the grid.

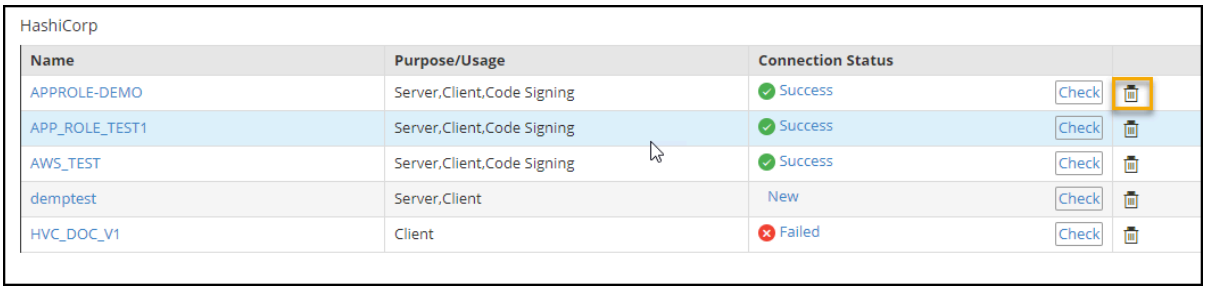
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



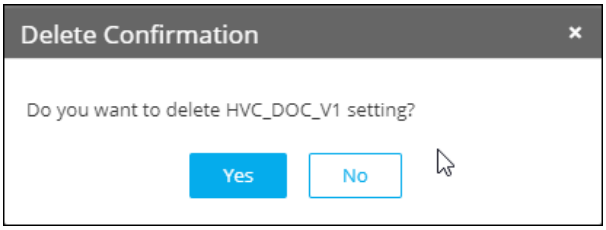
2. Click the account name from the ‘Name’ column in the grid.
   The General Information and CA Configuration sections are displayed with pre-populated values.
3. Change any of the editable fields and click the **Fetch Secret Engine** button.
4. Click the **Update** button.

Deleting an Account

1. Go to the **HashiCorp Vault** CA account home page
   The list of Accounts is displayed in the grid.



2. In the last column of the grid with the listed accounts, click the **Delete** or bin icon.
   The Delete Confirmation pop-up is displayed.



3. Click **Yes**.

Manually Validating the HashiCorp Vault CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **HashiCorp Vault**.
   The **HashiCorp Vault** home page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. In the Status column of the grid with the listed accounts, click the **Check** button.
   The Success or Failure value is displayed.
4. Update the account details accordingly to get a “success” status.

HydrantID CA

Prerequisites

To configure a HydrantID CA account in AppViewX, you will need:

- Base URL (already included in the AppViewX user interface)
- API key ID
- API key

  For links to detailed instructions to get the above information from HydrantID, see the **References** section.

  The API Key ID and API Key should be of the following user roles in HydrantID:
  - Account Auditor
  - Organization Admin
  - Organization Auditor
  - Requestor

  Once the organization (AppViewX) has subscribed for a HydrantID account, you will be provided with a **Username**, **Password**, and **Login URL** to create or update users/user roles.

  Users with role **Account Admin** in the HydrantID application can create the above roles. Only account admins can generate the API Key ID and API Key for the roles. Both values can be viewed for a limited time only. Ensure to note these values after the roles are added.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring HydrantID CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **HydrantID**.
   The **HydrantID** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The HydrantID CA details page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. Permissible special characters are '.', '-','_'. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Server, Client and Code-signing are the supported types.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the HydrantId APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain the hostname of the HydrantID CA instance and used for constructing the API requests. the default value is https://acm.hydrantid.com/api/v2
***API Key ID**	Enter the API Key ID generated in the HydrantID application. Its is a unique value specific to the user created in hydrant and is used to authenticate the user.
***API Key**	Enter the API Key generated in the HydrantID application. Its is a unique value specific to the user created in hydrant and used to authenticate and authorize requests.
**: Mandatory fields*	

6. Click **Fetch hydrantID policies**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A list of policies associated with the account are displayed. These are made available from HydrantID and are used for requesting different types of certificates.

Note: Configuration can only be saved in AppViewX if the profiles are available.

7. Update the following details in the **Advanced Settings** section as described in the table.

Advanced Settings - Field Description Table

Fields	Description
Poll after CSR Submission	A check box field when selected will fetch the certificated immediately after CSR Submission on enrollment, renew, and reissue of certificate with the retry count and retry frequency as described below.
***Retry Count**	The number of times the polling will take place after CSR submission. Enter a value between 1 and 10.
***Retry Frequency**	The duration of the polling. enter the value between 1 and 30seconds.
**: Mandatory fields*	

8. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

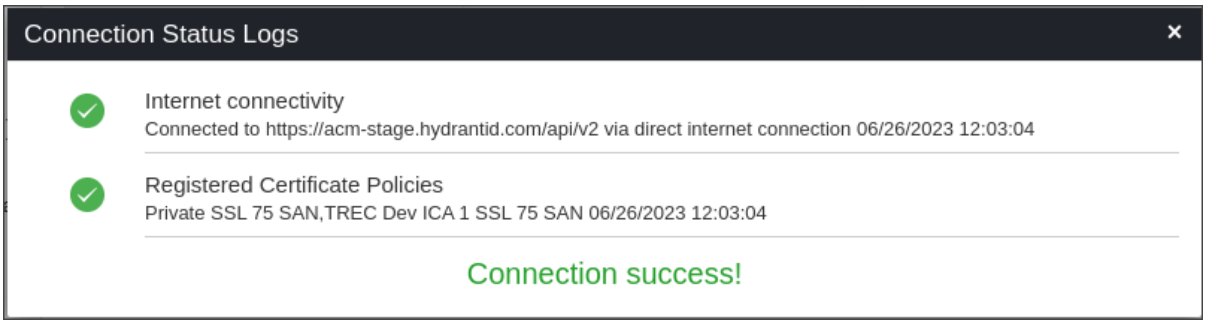
Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the HydrantID CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **HydrantID**.
   The **HydrantID** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**



References

Vendor documentation for retrieving HydrantID prerequisites:

- Managing API Keys

IDnomic CA

Prerequisites

To configure a IDnomic CA account in AppViewX, you will need:

- For the CA configuration:
  - CA Base URL
  - Partition name
  - Client authentication certificate
  - (Optional) SOAP signing authentication certificate

  To retrieve the above prerequisite values, please contact the IDnomic team. IDnomic will share these details via email or a shared file location.
- For the RA configuration:
  - RA base URL
  - RA client authentication certificate
  - Partition name

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To retrieve the above prerequisite values, please contact the IDnomic team. IDnomic will share these details via email or a shared file location.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Note: In the CA configuration page, if the checkbox **Use same certificate for signing SOAP requests** is selected, then **Client authentication certificate** is used as the **SOAP signing authentication certificate**.

Configuring IDnomic CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **IDnomic**.
   The **IDnomic** home page is displayed.
3. Click the **Configure Now** or **+Add** icon from the middle or top-right of the page respectively.
   The IDnomic configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table.

General Information - Field Description table

Fields	Description
***CA Account name**	A unique name to identify the CA setting No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example: Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Enter/Select the **CA Configuration** details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The IDnomic CA supports two configuration types:

- **CA** (Certificate Authority)

  In this configuration type, certificate discovery and CLM actions will be performed using certificate profiles configured in the Certificate Authority.

- **RA** (Registration Authority)

  In this configuration type, certificate discovery and CLM actions will be performed using RA workflows in the Registration Authority.

Field values entered/selected in the **CA Configuration** section define how AppViewX will connect with the IDnomic Certificate Authority (CA) or Registration Authority (RA).

CA Configuration - Field Description table

Fields	Description
Configuration Type	From the given options, select if AppViewX will connect with the IDnomic **CA** (Certificate Authority) or **RA** (Registration Authority). **Important:** Once selected, the **Configuration Type** for a CA setting cannot be changed. For field descriptions for configuring IDnomic CA in AppViewX with the CA setting, click here. For field descriptions for configuring IDnomic CA in AppViewX with the RA setting, click here.
**: Mandatory fields*	

Configuration Type = CA - Field Description table

Fields	Description
***CA Base URL**	Enter the base URL of the IDnomic CA API instance. For example: **https://ca-api-< >.axiadids.net/idca-server/services/soap/ca/2**
***Partition**	The name of the partition assigned to the organization's application. It is the workspace dedicated to the organization. The partitioning system allows implementing multi-tenancy within the IDnomic CA. Partitions

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	are defined in a tree structure, each node being a partitioning in which resources (e.g. Configurations, Certificate, etc) can be attached. According to the customer's needs we can isolate or share common resources.
***Client Certificate**	Upload the certificate for client authentication in the .p12 or .pfx format only.
SOAP Signing Required	If SOAP requests for certificate enrollment and revocation have to be digitally signed using the client certificate, turn on this setting. It is recommended to have this setting configured in accordance to the IDnomic CA portal.
Use same certificate for signing SOAP requests	To use the same certificate uploaded in the **Client Certificate** field for digitally signing the SOAP requests, select this checkbox.
***SOAP Signing Certificate**	This field is displayed only when the **Use same certificates for signing SOAP requests** option is disabled, which means a separate certificate (from the client certificate) has to be used for digitally signing the SOAP requests. Upload the certificate for soap signing authentication in the **.p12** or **.pfx** format only.
**: Mandatory fields*	

Configuration Type = RA - Field Description table

Fields	Description
***RA Base URL**	Enter the base URL of the IDnomic RA API instance. For example: **https://ra-api-< >.axiadids.net/idra-soap/soap/x509/ra/3.0**
***Partition**	The name of the partition assigned to the organization’s application. It is the workspace dedicated to the organization. The partitioning system allows implementing multi-tenancy within the IDnomic RA. Partitions are defined in a tree structure, each node being a partitioning in which resources (e.g. Configurations, Certificate, etc) can be attached. According to the customer's needs we can isolate or share common resources.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***RA Client Certificate**	Upload the certificate for RA client authentication in the **.p12** or **.pfx** format only.
**: Mandatory fields*	

6. Depending on the **Configuration Type** selected, click **Fetch Certificate Profiles/Fetch RA Workflows**.
   If **Configuration Type** = **CA**, the complete list of certificate profiles is displayed.

   If **Configuration Type** = **RA**, the complete list of RA workflows is displayed.
7. Click **Save**.
   The confirmation message **Certificate profiles fetched successfully/RA workflows fetched successfully** (depending on the selected configuration type) is displayed and the CA is created successfully.

   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

   Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the IDnomic CA Connection Status

1. Go to **(Menu) > CERT+ > ADMINISTRATION > Certificate Authority.**
2. From the displayed CA, Select **IDnomic**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the Connection Status will be shown as either Success or Failure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Figure 1. RA Validation

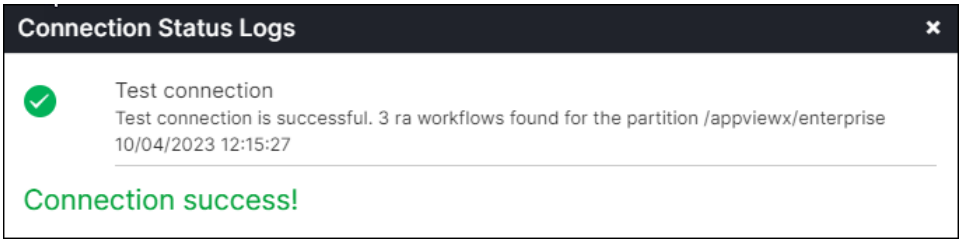
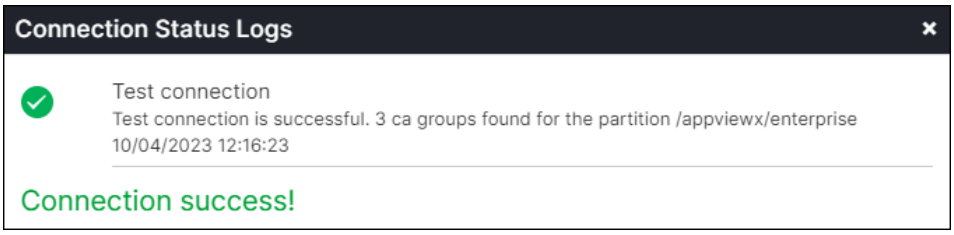


Figure 2. CA Validation



Known Limitations

Due to IDnomic API limitations, AppViewX is not notified when a certificate revocation request is declined. Hence, work orders for certificate revocation may still be shown as failing even if they are declined. This limitation will be addressed in the subsequent release versions.

InCommon CA

Prerequisites

To configure a InCommon CA account in AppViewX, you will need:

- Base URL and login URL
- Username and password for the following roles:
  - Master Registration Authority Officer
  - Registration Authority Officer
- Requisite credentials with access to certificate enrollment for InCommon Certificate Manager
- Organization ID

  For links to detailed instructions to get the above information from InCommon, see the **References** section.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring InCommon CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **InCommon**.
   The **InCommon** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **InCommon** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Purpose/ Usage**	Certificate Type for which CLM actions will be enabled. Eg. Server, Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the InCommon CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	This URL will contain just the hostname of the InCommon CA instance. Eg -https://cert-manager.com/customer/<<customer_uri>>/ssl- here base URL is **https://cert-manager.com.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Login URL**	URI specific to the InCommon CA Customer Account. Eg https://cert-manager.com/customer/<<customer_uri>>/ssl- here URI is **customer_uri**.
***User Name**	User name for the account created with InCommon CA.
***Password**	Password for the account created with InCommon CA.
***Organization ID**	InCommon supports organization hierarchy. Id of the **Organization Unit/ Department** in which Certificates need to be managed has to be specified here. **CLM** actions done using this CA account will be specific to this particular organization's id/department.
**: Mandatory fields*	
Note: If the certificates from multiple organization's units/departments need to be managed, then a separate CA has to be configured for each organization unit/department in the Incommon CA setting page.	

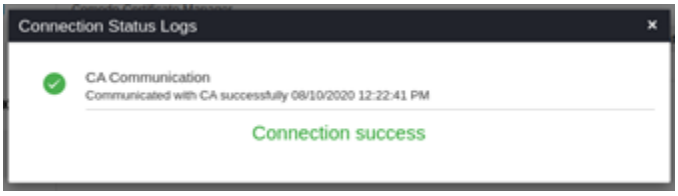
6. Select **Fetch Certificate Types**
   The Certificate types available for the CA account will be fetched from the Certificate Authority.
7. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Manually Validating the InCommon CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **InCommon**.
   The **InCommon** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



References

Vendor documentation for retrieving InCommon prerequisites:

Download the InCommon Certificate Manager Quick Start Guide.

In this PDF:

- For the base URL and login URI, refer the section to **Log in to InCommon CM**.
- To create an oragnization, refer the section to **Create Organizations and Departments**. Once you've created an organization, InCommon will assign you an organization ID.

  To review the organization details in the SCM, navigate to **Organizations**, select the organization in the list, and click **Edit**. This displays the **Edit Organization** dialog box.
- To create administrator roles, such as MRAO and RAO, refer the section to **Add Administrators**.

  Ensure that these roles have the following privileges:

Privileges	
Allow SSL details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to Certificates > SSL Certificates.
Allow SSL auto approve	SSL certificates requested by the MRAO are automatically approved, and those requested by a RAO SSL and DRAO SSL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Privileges	
	are automatically approved by the administrator of same level and await approval from higher level administrator.

To review the administrator details in the SCM, navigate to **Settings > Admins**, select the administrator in the list, and click **Edit**. This displays the Edit Client Admin dialog, Add/Edit the necessary privileges and click **Save**.

Let's Encrypt CA

Prerequisites

To configure a Let's Encrypt CA account in AppViewX, you will need:

- One of the following Let's Encrypt base URLs for certificate enrollment, as required:
  - Staging URL
  - Production URL

  For links to detailed instructions to get the above information from Let's Encrypt, see the **References** section.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring Let's Encrypt CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Let's Encrypt**.
   The **Let's Encrypt** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The Let's Encrypt configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

General Information - Field Description Table

Fields	Description
***Name**	A unique name to identify the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Purpose/Usage**	The certificate types will be managed by these settings. For now, Let's Encrypt is having only one purpose **Server**.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Let's Encrypt CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	Let's Encrypt certificate enrolment URL either staging or production based on the requirement.
***Email ID(s)**	Enter email ID(s) in this field to receive notifications from Let's Encrypt. Multiple email ID must be separated by comma (,).
**: Mandatory fields*	

6. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Manually Validating the Let’s Encrypt CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Let's Encrypt**.
   The **Let's Encrypt** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

References

Vendor documentation for retrieving Let's Encrypt prerequisites:

- Staging URL
- Production URL

Microsoft Enterprise CA

Prerequisites

To configure a Microsoft Enterprise CA account in AppViewX, you will need:

- AppViewX Windows Gateway installer installed on a Windows machine, running and reachable from the AppViewX vendor plugin through the communication modes described here.
- **Windows Gateway URL**: It is the registered gateway URL of the server where the windows gateway is hosted/installed. The URL format is **https://hostname:portnumber/appviewx**. For example: https://10.10.10.10:8999/appviewx
- **Client Authentication Certificate**: It is the certificate (.p12 or .pfx format) that is shipped with the windows gateway agent installer.

  The Windows Gateway URL and the client authentication certificate will be made available only after installation of the AppViewX Windows Gateway is incomplete. Refer the AppViewX Windows Gateway Setup documentation here.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Microsoft Enterprise CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Enterprise** tab.
4. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
5. Enter/Select the CA **General Information**.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. Example. Server, Client, Code Signing
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Enter/Select the **CA Configuration** details.

CA Configuration - Field Description Table

Fields	Description
Windows Gateway Mode	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• **Integrated** This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode
***Windows Gateway URL**	For **Windows Gateway Mode** = **External**, enter the URL of the endpoint where the AppViewX Windows Gateway Agent is installed and running.
Command Execution Type	Select the command type that will be used for communication with the External AppViewX Windows Gateway Agent. **Note:** The integrated gateway uses only the PowerShell command execution type and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
Command execution host (IP/FQDN)	**Note:** This field is displayed when **Windows Gateway Mode** = **Integrated**. A command execution host is a Windows device needed to execute specific commands to fetch the CAs and templates available. The command execution host is expected to be a domain controller machine (primary) and will be used only once to fetch the list of available CAs. Enter the IP address/FQDN of the remote Windows device that the integrated gateway will use for CA communication. **Note:** If the Microsoft server is configured for the **Integrated Windows Gateway** mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
***Credential Type**	You will be required to enter credentials to access the command execution host/Windows device on which the gateway agent is running.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	From this dropdown list, select the mode through which the credentials will be entered (manually or fetched from a credential list).
***Username**	Enter the username for accessing the Windows device.
***Password**	Enter the password for accessing the Windows device.
Client Authentication Certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

7. Click **Fetch CA Names** to retrieve CAs accessible from Windows Gateway installed machine. Upon successful completion of Fetch CA Names, all reachable CAs listed in **Select CA**.
8. Click on one specific CA and proceed.

CA Details - Field Description Table

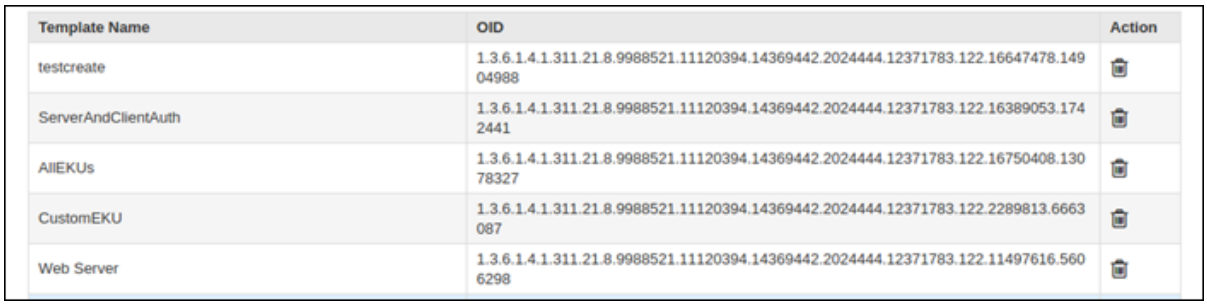
Fields	Description
Select CA	All the reachable CAs are listed here.
***CA Machine Hostname**	Host name of the CA Machine will be auto-filled. **Note:** • If the Microsoft server is configured for the **Integrated Windows Gateway** mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred. • The credentials used for Fetch CA will also be utilized for CA machine communication through the Integrated Gateway.
***CA Name**	Name of the CA chosen which will be auto-filled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
CA Manager Approval	Approves the pending enroll / Renew request submitted from AppViewX Certificate.
***Time Zone**	To perform scheduled and Optimized CA discovery, please provide time zone value.
**: Mandatory fields*	

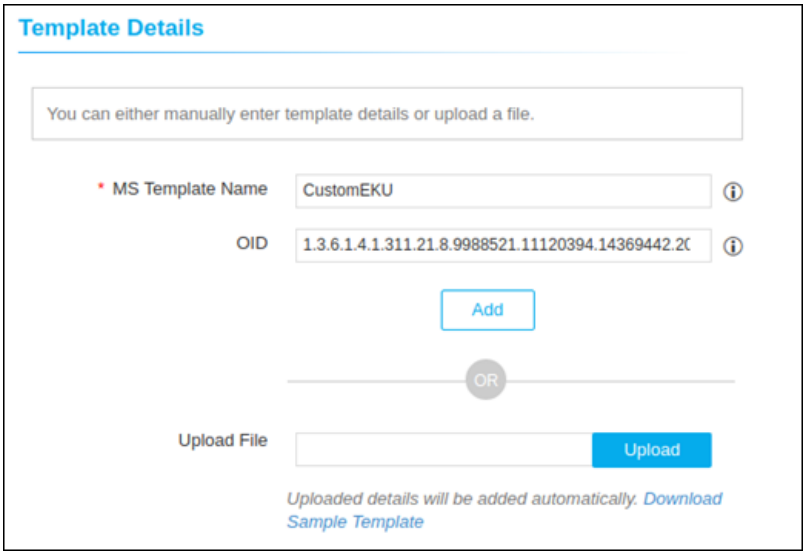
a. Configure the **Template Details**.

Once CA is selected from the **Select CA** list, the **Template** details should have auto-filled as shown below.



Note: If the desired template is not listed, it might not be published in AD. Users can add it manually through MS Template name and OID fields as shown below.

b. In the Template Details section, select/enter the details as shown below.



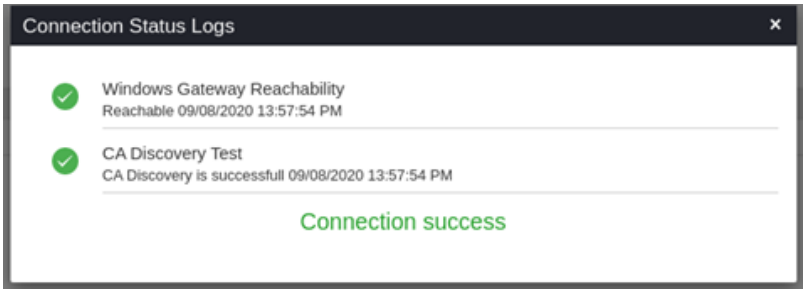
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Click **Save.**
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

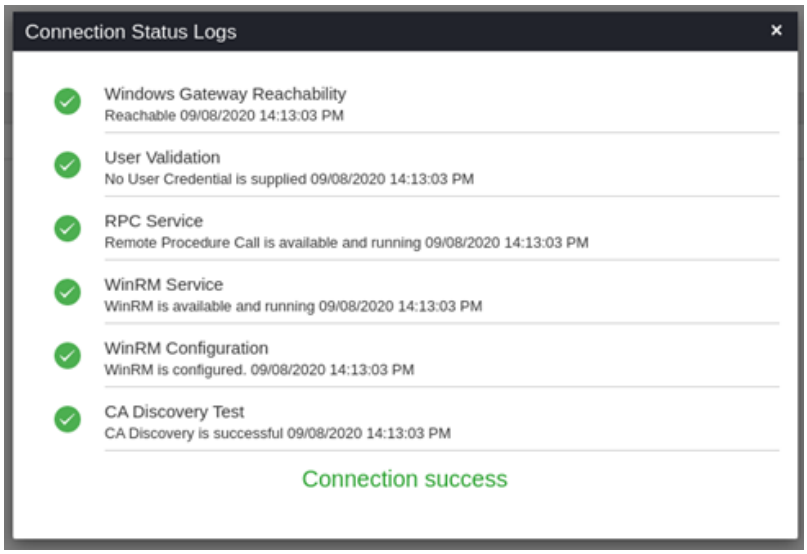
Manually Validating the Microsoft Enterprise CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Enterprise** tab.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

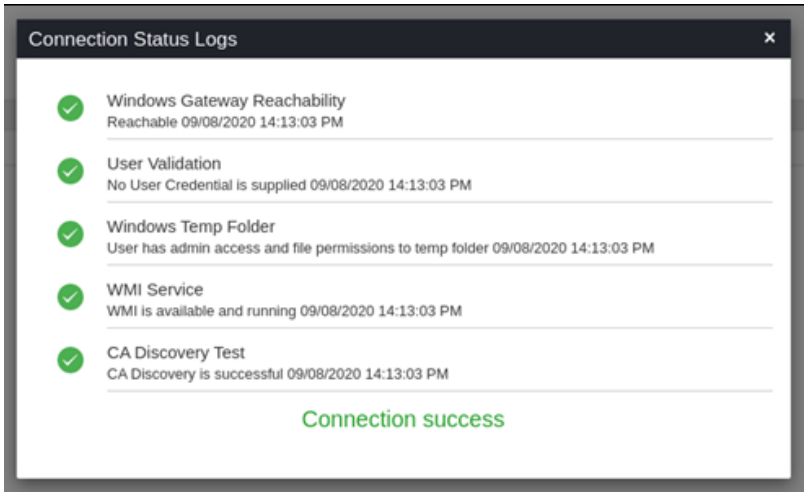


Success Scenario for Native API

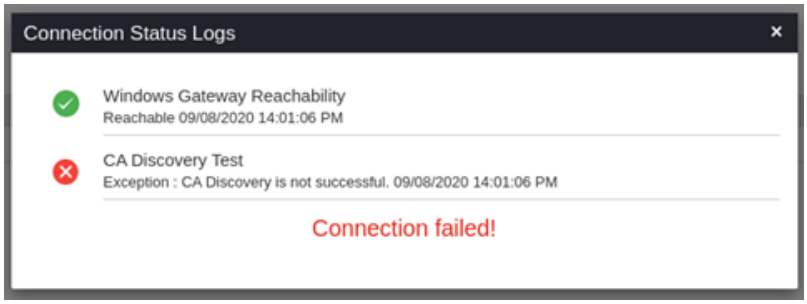
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Success Scenario for Powershell



Failure scenario for WMI



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Communication Modes

Communication Mode Table

Communication mode	Category	Windows gateway machine	Microsoft CA
NATIVE API	User account type	Service account	Service account.
	User permission	NA	Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users Enroll permission at Certificate template level for the service account or the service account group or authenticated users
	Services	RPC service	RPC service certutil.exe command availability
	Ports	49152-65535	49152-65535
POWERSHELL	User account type	Service account	Admin account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	RPC Service, WinRM Service, WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service, WinRM Service, WinRM Configuration, Powershell remoting,certutil.exe command availability.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Communication Mode Table (continued)

Communication mode	Category	Windows gateway machine	Microsoft CA
	Ports	NA	5985
WMI	User account type	Service account	Admin account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	WMI service certutil.exe command availability	WMI service certutil.exe command availability
	Ports	49152-65535.	49152-65535

Microsoft Standalone CA

Prerequisites

To configure a Microsoft Standalone CA account in AppViewX, you will need:

- AppViewX Windows Gateway installer installed on a Windows machine, running and reachable from the AppViewX vendor plugin through the communication modes described here.
- **Windows Gateway URL**: It is the registered gateway URL of the server where the windows gateway is hosted/installed. The URL format is **https://hostname:portnumber/appviewx**. For example: https://10.10.10.10:8999/appviewx
- **Client Authentication Certificate**: It is the certificate (.p12 or .pfx format) that is shipped with the windows gateway agent installer.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The Windows Gateway URL and the client authentication certificate will be made available only after installation of the AppViewX Windows Gateway is incomplete. Refer the AppViewX Windows Gateway Setup documentation here.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring Microsoft Standalone CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Standalone** tab.
4. In the Status column of the grid with the listed accounts, click and then click **+Add** icon or **Configure Now** button.
5. Enter/Select the CA **General Information**.

General Information - Field Description Table

Fields	Description
Name	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example: Server, Client, and Code Signing.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

6. Enter/Select the **CA Configuration** details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Configuration - Field Description Table

Fields	Description
Windows Gateway Mode	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode
***Windows Gateway URL**	For **Windows Gateway Mode** = **External**, enter the URL of the endpoint where the AppViewX Windows Gateway Agent is installed and running.
Command Execution Type	Select the command type that will be used for communication with the External AppViewX Windows Gateway Agent. **Note:** The integrated gateway uses only the PowerShell command execution type and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
Command execution host (IP/FQDN)	**Note:** This field is displayed when **Windows Gateway Mode** = **Integrated**. A command execution host is a Windows device needed to execute specific commands to fetch the CAs and templates available. The command execution host is expected to be a domain controller machine (primary) and will be used only once to fetch the list of available CAs. Enter the IP address/FQDN of the remote Windows device that the integrated gateway will use for CA communication.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If the Microsoft server is configured for the **Integrated Windows Gateway** mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
***Credential Type**	You will be required to enter credentials to access the command execution host/Windows device on which the gateway agent is running. From this dropdown list, select the mode through which the credentials will be entered (manually or fetched from a credential list).
Username	Enter the username for accessing the Windows device.
Password	Enter the password for accessing the Windows device.
Client Authentication Certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

7. Click **Fetch CA Names** to retrieve CAs accessible from Windows Gateway installed machine. Upon successful completion of Fetch CA Names, all reachable CAs listed in **Select CA**.
8. Click on one specific CA and proceed.

Dynamic Fields for Select CA Section

Fields	Description
Select CA	All the reachable CAs are listed here.
***CA Machine Hostname**	Host name of the CA Machine will be auto-filled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If the Microsoft server is configured for the **Integrated Windows Gateway** mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred. • The credentials used for Fetch CA will also be utilized for CA machine communication through the Integrated Gateway.
***CA Name**	Name of the CA chosen which will be auto-filled.
CA Manager Approval	Approves the pending enroll / Renew request submitted from AppViewX Certificate.
**: Mandatory fields*	

9. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

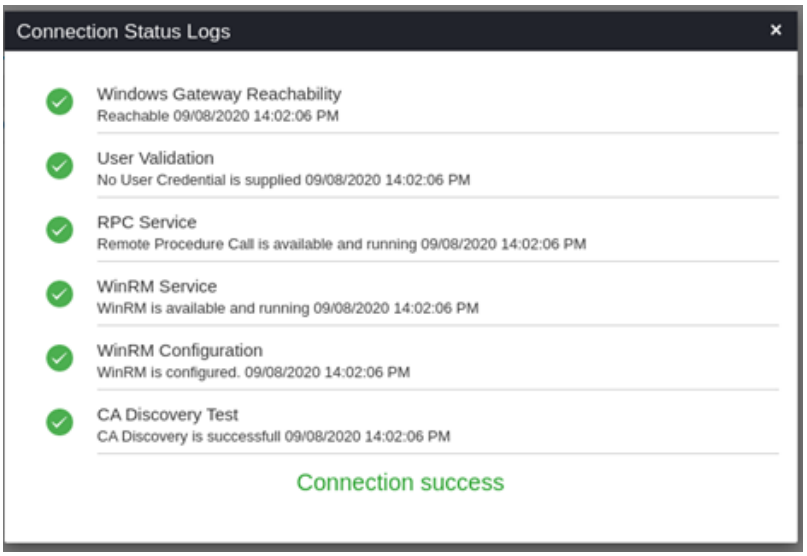
Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Microsoft Standalone CA Connection Status

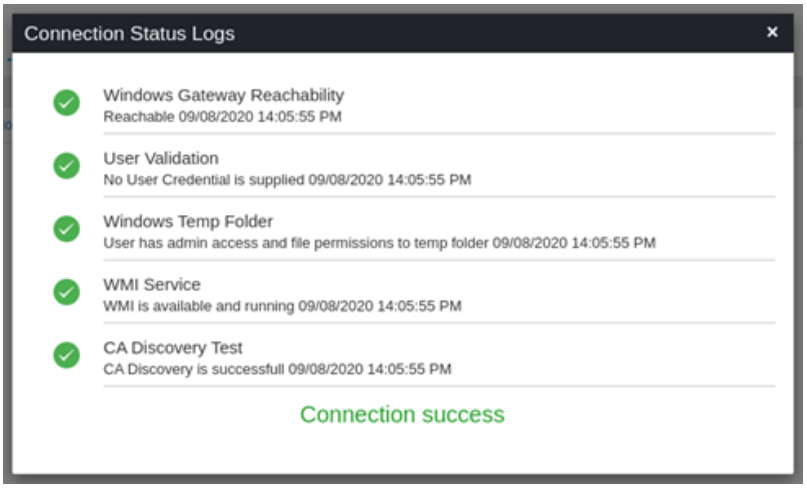
1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Microsoft**.
   The **Microsoft** home page is displayed.
3. Select the **Standalone** tab.
4. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.Success scenario for Native APISuccess scenario for PowershellSuccess scenario for WMI.

   Success scenario for Native API

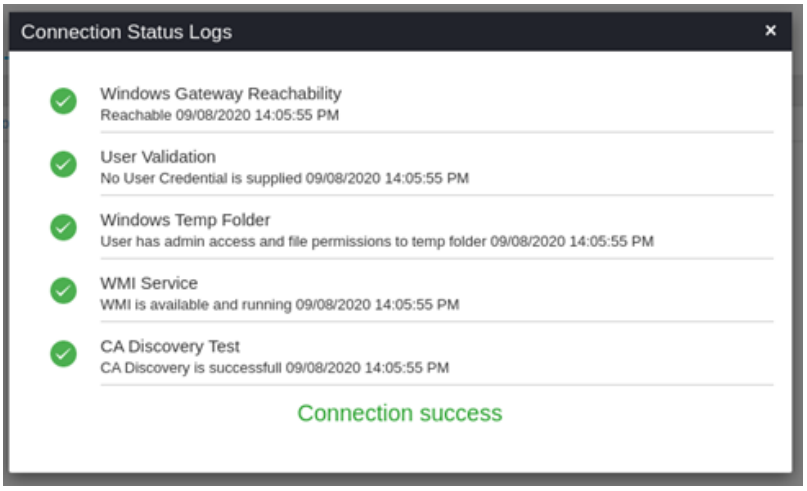
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Success scenario for Powershell



Success scenario for WMI



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Communication Modes

Communication Mode Table

Communication mode	Category	Windows gateway machine	Microsoft CA
NATIVE API	User account type	Service account	Service account.
	User permission	NA	Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users Enroll permission at Certificate template level for the service account or the service account group or authenticated users
	Services	RPC service	RPC service certutil.exe command availability
	Ports	49152-65535	49152-65535
POWERSHELL	User account type	Service account	Admin account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	RPC Service, WinRM Service, WinRM Configuration, Powershell remoting,certutil.exe command availability	RPC Service, WinRM Service, WinRM Configuration, Powershell remoting,certutil.exe command availability.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Communication Mode Table (continued)

Communication mode	Category	Windows gateway machine	Microsoft CA
	Ports	NA	5985
WMI	User account type	Service account	Admin account
	User permission	NA	Full control permission to C:\Windows \Temp Read, Request certificates, Issue and Manage certificates permission at CA level for the service account or the service account group or authenticated users
	Services	WMI service certutil.exe command availability	WMI service certutil.exe command availability
	Ports	49152-65535.	49152-65535

Nexus CA

Prerequisites

To configure a Nexus CA account in AppViewX, you will need:

- Base URL
- Client certificate, for communication between AppViewX and Nexus
- Organization ID

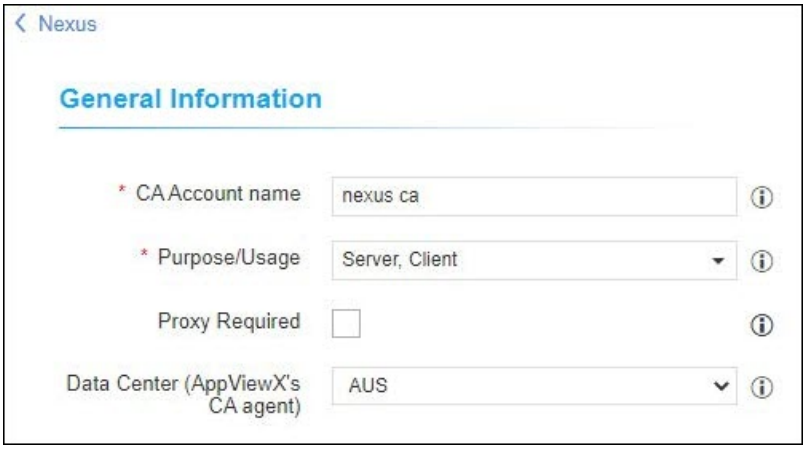
  Please contact the Nexus team for retrieving the above listed prerequisite values.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.
- CA certificates manually uploaded before certificate discovery or enrollment is initiated

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Nexus

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Nexus**.
   The **Nexus** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The Nexus configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table.

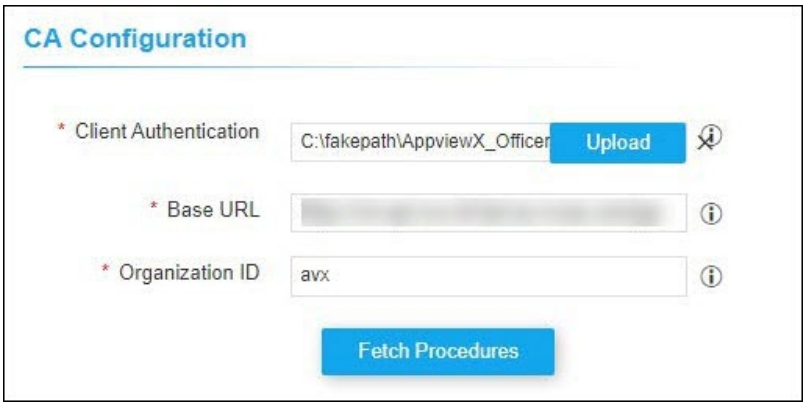


General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, server and clients
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

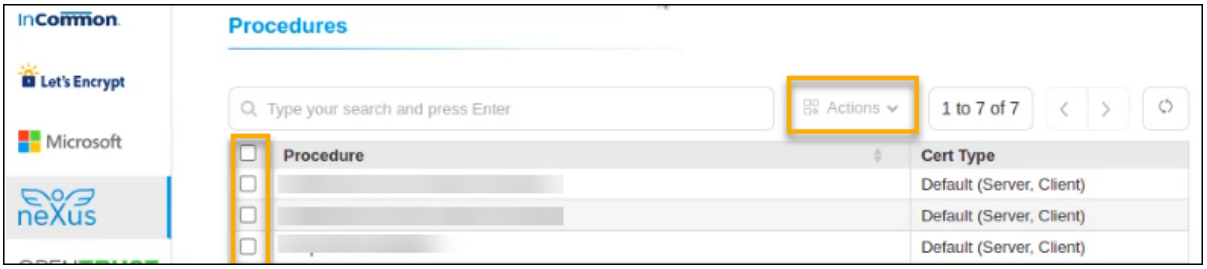


CA Configuration - Field Description Table

Fields	Description
***SSL URL**	Base URL of the SSL API
***User Name**	Provide a username of the GCC to communicate with the CA.
***Password**	Provide a password for the GCC to communicate with the CA.
**: Mandatory fields*	

6. Select **Fetch Procedures**.

   The procedures available in the Nexus CA account will be fetched and listed for the specific user.



7. To map the fetched procedures, click on one or many and click the **Actions** dropdown
   - **CASE 1** - If the user selects Server only in Purpose and Usage, then the fetched procedure by default will be of server/client both. The Action dropdown will only have - **Map as Server**. and **MAP as Default**
   - **CASE 2** - If the user selects Client only in Purpose and Usage, then the fetched procedure by default will be of server/client both. The Action dropdown will only have - **Map as Client**. and **MAP as Default**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

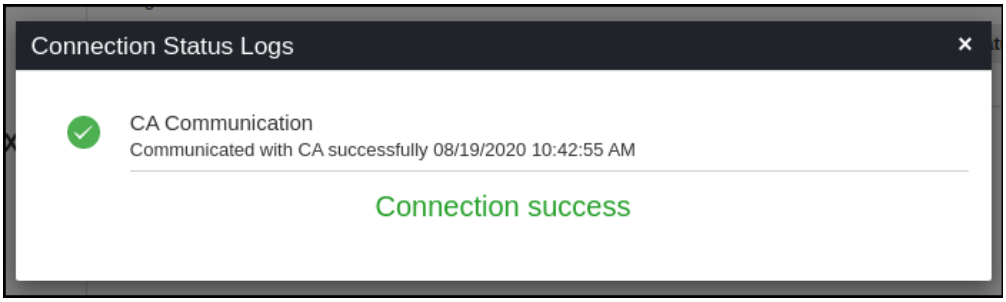
- **CASE 3** - If the user selects Server and Client both in Purpose and Usage, then the fetched procedure by default will be of server/client both. The Action dropdown will have both the actions **Map as Client** , **Map as Server**, and **MAP as Default**

8. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Nexus CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Nexus**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the Connection Status will be shown as either Success or Failure.



Sectigo CA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

To configure a Sectigo CA account in AppViewX, you will need:

- Base URL and login URI
- Username and password for the following roles:
  - Master Registration Authority Officer
  - Registration Authority Officer
- Organization ID

  For links to detailed instructions to get the above information from Sectigo, see the **References** section.
- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring Sectigo CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the list of CAs displayed on the left, select **Sectigo**.
   The **Sectigo** CA account inventory is displayed.
3. If it is your first DigiCert CA integration in AppViewX, click **Configure Now**.
   The **Configure Now** button is displayed only if this is the first integration instance.

   For the subsequent integrations, from the top-right corner of the page, click **Add**.

   The **Sectigo** configuration page is displayed.
4. Enter/Select the **General Information** details for the Sectigo CA configuration.

General Information - Field Description Table

Fields	Description
***CA Account name**	Enter a unique name for the Certificate Account (CA) account, which will be displayed during certificate enrollment and policy creation. **Constraints**: • Valid special characters: **.**, **-**, and _ • CA account name should not begin with a special character and/or a space.
***Purpose/Usage**	From the dropdown list, select the certificate type(s) for which CLM actions will be enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Possible values: Server, Client
Proxy Required	For CA communication to happen via a proxy, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
Data Center (AppViewX's CA agent)	From the dropdown list, select the data center through which the CA communication must happen.
**: Mandatory fields*	

5. To invoke the Sectigo CA APIs for certificate management, enter/select the **CA Configuration** details.

CA Configuration - Field Description Table

Fields	Description
***Base URL**	Enter the base URL for constructing the API requests. The URL will contain the hostname of the Sectigo CA instance.
***Login URI**	Enter the login URI for your Sectigo CA account for API authentication.
***Authentication Method**	To connect to the certificate authority, select an authentication method from the following options: • **Password**: A text-based credential will be used to verify identity and authenticate the connection to the CA. • **Client Certificate**: A digital certificate issued to the user is used to authenticate identity securely by validating the certificate.
***User Name**	Enter the Sectigo portal username to communicate with the CA.
***Password**	**Note:** This field is displayed when **Authentication Method** = **Password**. Enter Sectigo portal password to communicate with the CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Client Certificate**	**Note:** This field is displayed when **Authentication Method** = **Client Certificate**. Upload the client authentication **.pfx** file to communicate with the CA. To do this: a. Click **Upload** and navigate to the location of the certificate file. b. Select the required certificate file. The **Authentication Details** dialog box is displayed. c. In the **Enter Password** field, enter the selected certificate file's password and click**OK**. **Note:** Ensure that the end entity has access to enroll a certificate with the required CA.
***Organization ID**	Enter the organization ID used for the certificate lifecycle action. (You will find it in the **Organization** tab of the Sectigo portal.)
**: Mandatory fields*	

6. To fetch the certificate types assigned for you, click **Fetch Certificate Types**.
   AppViewX connects to Sectigo using the authentication method selected and fetches the certificate types based on the **Purpoe/Usage** selected. These certificate types will the be used throughout the product for certificate enrollment and policy creation.
7. Enter/Select the **Advanced Settings** for polling Sectigo after the CSR request is submitted.
   These settings ensure that AppViewX is efficiently and regularly checking for certificate issuance status (after CSR submission for enrollment/renewal/reissue requests) without sending excessive API requests to the CA.

Advanced Settings - Field Description Table

Fields	Description
Poll after CSR Submission	To enable AppViewX to automatically poll Sectigo after CSR submission, select this checkbox.
***Retry Count**	This field is displayed only when **Poll after CSR submission** is selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the number of times AppViewX will retry polling Sectigo before it stops. For example, if **Retry Count** = 5, AppViewX will poll Sectigo 5 times before it stops. **Possible values**: Between 1 and 10
***Retry Frequency**	This field is displayed only when **Poll after CSR submission** is selected. Enter the interval (in seconds) between attempts. For example, if **Retry Frequency** = 10, AppViewX will wait for 10 seconds between each polling attempt. **Possible values**: Between 1 and 30 seconds
**: Mandatory fields*	

8. Click **Fetch Custom Attributes**.
   Custom attributes defined for the CA account will be fetched from the CA along with the CA and profile names. On successful retrieval, the message **CA and profiles fetched** is displayed.
9. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

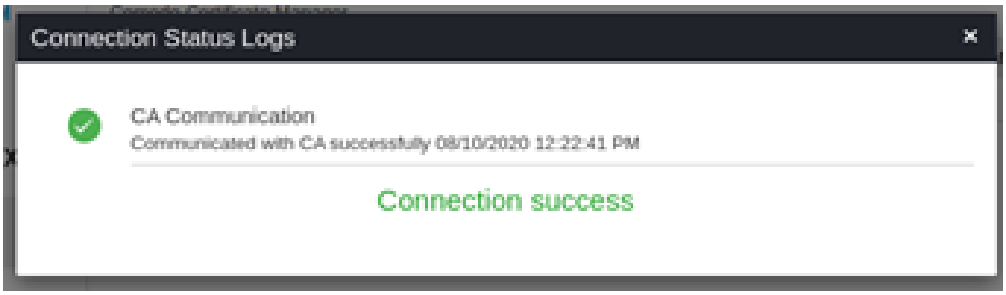
> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Sectigo CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Sectigo**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.



References

Vendor documentation for retrieving Sectigo prerequisites:

Download the Sectigo Certificate Manager Quick Start Guide.

In this PDF:

- For the base URL and login URI, refer the section on **Logging in to SCM**.
- To create an oragnization, refer the section on **Adding organizations and departments**. Once you've created an organization, Sectigo will assign you an organization ID.

  To review the organization details in the SCM, navigate to **Organizations**, select the organization in the list, and click **Edit**. This displays the **Edit Organization** dialog box.
- To create administrator roles, such as MRAO and RAO, refer the section on **Adding Administrators**.

  Ensure that these roles have the following privileges:

Privileges	
Allow SSL details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to Certificates > SSL Certificates.
Allow SSL auto approve	SSL certificates requested by the MRAO are automatically approved, and those requested by a RAO SSL and DRAO SSL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Privileges	
	are automatically approved by the administrator of same level and await approval from higher level administrator.

To review the administrator details in the SCM, navigate to **Settings > Admins**, select the administrator in the list, and click **Edit**. This displays the Edit Client Admin dialog, Add/Edit the necessary privileges and click **Save**.

SwissSign CA

Prerequisites

To configure a SwissSign CA account in AppViewX, you will need:

- CA Base URL
- Username
- API key

The SwissSign team manages user creation and access controls for users. Users must have a level of **RAO (Registration Authority Officer)** or higher to perform actions like issuing, revoking, updating, and viewing certificates.

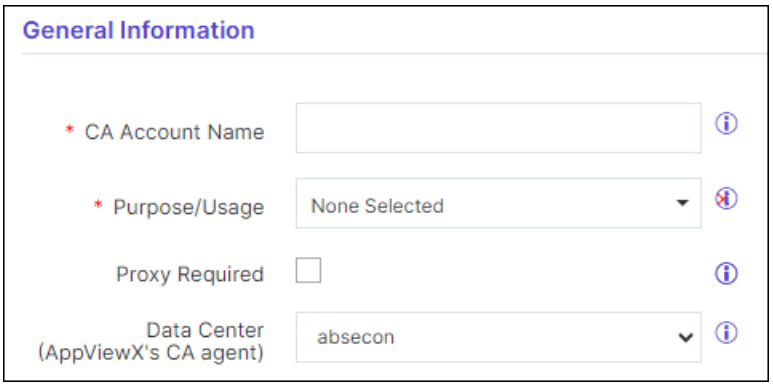
For links to detailed instructions to get the above information from Sectigo, see the **References** section.

- Internet access or a proxy configuration for the AppViewX server. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring SwissSign CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, Select **SwissSign**.
   The **SwissSign** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **SwissSign CA** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

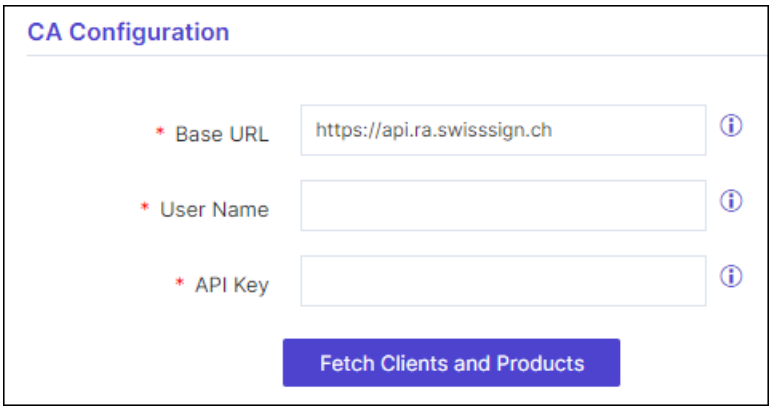


General Information - Field Description Table

Fields	Description
***CA Account name**	Enter a unique name in the text field to identify the CA account and be represented during certificate enrollment and policy creation. No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Select the purpose of the certificate from the dropdown list for which CLM actions will be enabled. Example: Server, Client
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
*: *Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the CSC Global CA APIs for Certificate Management:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

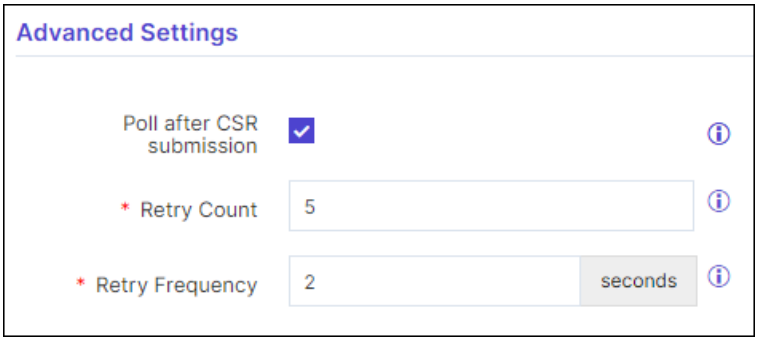


CA Configuration - Field Description Table

Fields	Description
***CA Base URL**	Enter the base URL that will be used to construct the API request. The value is *https://api.ra.swisssign.ch*
***Username**	Enter the service account username to communicate with the RA.
***API Key**	Enter the API key which is a unique identifier used to authenticate the user. The value entered will be masked and encrypted.
*: *Mandatory fields*	

6. Click **Fetch Clients and Products.**

   If the data provided is accurate the success message “Clients and Products fetched successfully“ will be displayed and a table is displayed with two columns - *Client* and *Product Name* (the product name is similar to the certificate profile).
7. Update the following details in the **Advanced Settings** section as described in the table.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Advanced Settings - Field Description Table

Fields	Description
***Poll after CSR submission**	Selecting the checkbox enables polling after CSR submission. It fetches the certificates immediately after CSR submission on enrollment, renew, and reissue with the retry count and retry frequency specified in the fields below.
***Retry Count**	Enter a value between 1 - 10.
***Retry Frequency**	Enter a value between 1 - 30 seconds.
*: *Mandatory fields*	

8. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case **Fetch Clients and Products** is not triggered before saving CA settings, this action can explicitly perform both these actions and update the CA.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the SwissSign CA Connection Status

1. On the SwissSign CA page, the above configured CA will be displayed with a **Check** button in the last column of the table.
2. Click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

References

Vendor documentation for retrieving SwissSign prerequisites:

Download the SwissSign CA RA Operator Manual.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

In this PDF:

- For the CA base URL, refer the section on **Login with SwissID**.
- For the account username, refer the section on **Account details**.
- For the API key, refer the section on **Service API keys**.

Symantec CA

Prerequisites

The prerequisites for configuring a Symantec account in AppViewX are as follows:

- A Symantec client certificate for a user having the necessary access for enrolling the certificates and other Certificate Lifecycle Management(CLM) operations.
- AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Refer to the section Managing Proxy Settings in the Platform guides.
- Symantec users should be associated with the role **“w=VICE2 web services application”**.
- Required organization status should be “valid”.
- If the EV certificate type is enabled, then the EV status of the organization should be “Yes”.
- The required domain should be registered with the organization.
- The required certificate types should be enabled with the required values in the portal.
- Unit values should be available for the required certificate type.

Configuring Symantec CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Symantec**.
   The **Symantec** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The **Symantec** configuration page is displayed.
4. Update the following details in the **General Information** section as described in the table.

General Information - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. The name must not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server and Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen.
**: Mandatory fields*	

5. Update the following details in the **CA Configuration** section as described in the table. These fields are necessary for invoking the Symantec CA APIs for Certificate Management.

CA Configuration - Field Description Table

Fields	Description
***Certificate and Key**	Client authentication certificate for API communication. **Note:** Certificate must be a valid <.p12> or <.pfx> file.
***URL**	Symantec URL used for API communications. For example, **https://certmanager-webservices.websecurity.symantec.com/vswebservices/**
***Jurisdiction hash**	Jurisdiction hash of the Symantec account. Available in the top right corner of the Symantec portal.
***First name**	First name of the user.
***Last name**	Last name of the user.
**: Mandatory fields*	

6. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

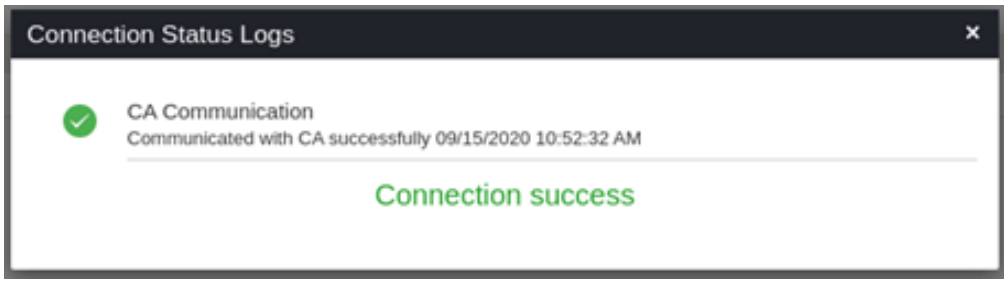
In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

Note: In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

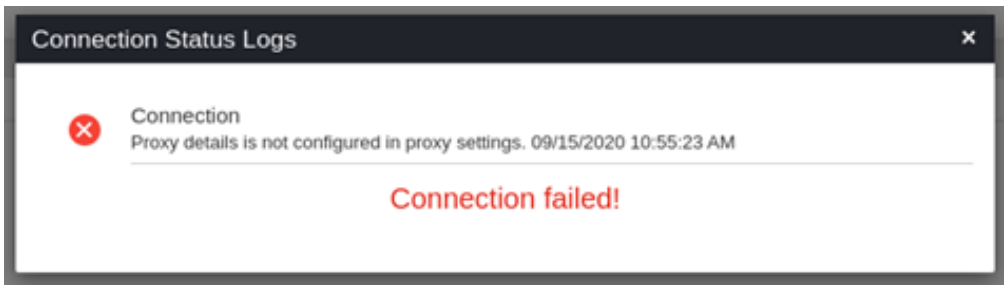
Manually Validating the Symantec CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Symantec**.
   The **Symantec** home page is displayed.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that has been created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

Success Scenario



Failed Scenario



Trustwave CA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

The prerequisites for configuring Trustwave CA account in AppViewX are as follows:

- Trustwave **API URL**. Ex: https://testapi.ssl.trustwave.com/3.0/.
- Valid credentials for communicating to Trustwave CA via API. The **Username** and **Password** are emailed when your account is set up by Trustwave. Additionally, users with admin access can create accounts in Trustwave by the following steps:
  1. Login to your Trustwave account and navigate to **Account Management** > **Manage Users**.
  2. Click **+Add User**
  3. In the **Add a User** pop-up, enter the relevant details and click **Add User**.

  Note: While assigning User Roles, minimum permissions are applicable to **View** and **Request** roles, and maximum permission are applicable to **Administer** and **Scan** roles.

- The **Reseller Id** is an identifier assigned by Trustwave that uniquely identifies each customer's account.
- Account details provided in Trustwave account such as Organization Name, Email address, Organization Address, City, State, Zip code, Country, and Phone number. (Details are available in your Trustwave account, **Account Management** > **My Account**.
- Reachability from AppViewX southbound to Trustwave API URL via proxy or direct internet connection. AppViewX server should either have internet access or have a proxy configured in AppViewX general settings. Refer to the section Managing Proxy Settings in the Platform guides.

Configuring Trustwave CA

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Trustwave**.
   The **Trustwave** home page is displayed.
3. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
   The Trustwave CA details page is displayed.
4. Configure the **General Information** details as follows:

General Information - Field Description Table

Fields	Description
***CA Account name**	Provide an account name for the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Purpose/Usage**	Choose the certificate categories that will be managed by this setting. Possible certificate categories could be: a. Server b. Code Signing
Proxy Required	Enable this field if the CA communication needs to happen via **Proxy**.
Data Center (AppViewX's CA agent	Choose the appropriate **Data Center**.
**: Mandatory fields*	

5. Configure the **CA Configuration** with information you want to configure:

CA Configuration - Field Description Table

Fields	Description
***API URL**	The Trustwave API URL to communicate. E.g.: https://testapi.ssl.trustwave.com/3.0/
***Username**	The username for API authentication.
***Password**	The password for API authentication.
***Reseller ID**	The Reseller Id for the account. An identifier assigned by Trustwave that uniquely identifies each customer's account.
**: Mandatory fields*	

6. Configure the **Account Details** with information you want to configure:

CA Configuration - Field Description Table

Fields	Description
***Name**	The Organization name given in the Trustwave account.
***Email Address**	The Administrator or organization email address given in the Trustwave account.
***Address**	The Organization Address given in the Trustwave account.
***City**	The city name given in the Trustwave account.
***State**	The state name given in the Trustwave account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Zip code**	The zip code given in the Trustwave account.
***Country**	The country code given in the Trustwave account. E.g.: US.
***Phone number**	The phone number given in the Trustwave account.
**: Mandatory fields*	

7. Click **Save**.
   In the CA instance inventory, the connection status is initially set to **In Progress**. Twice after this, this status is automatically checked and refreshed every 5 seconds. Once the CA instance is successfully configured, the status is updated to **Success**. Status checks after the first two times have to be done via a manual refresh.

> **Note:** In case the connection fails, you can manually verify the connection status by clicking the **Check** button in the **Connection Status** field.

Manually Validating the Trustwave CA Connection Status

1. Go to **(Menu)** > **CERT+** > **ADMINISTRATION** > **Certificate Authority**.
2. From the displayed CA, select **Trustwave**.
3. In the Status column of the grid with the listed accounts, click **Check** to validate the CA setting that is created.
   The CA communication will be validated and the **Connection Status** will be shown as either **Success** or **Failure**.

CA Policy

You can enforce your organization standards by configuring **Certificate Policy** in **CERT+**. Thus the attributes of discovered certificates are compared against the certificate policy to ensure they are complaint. If the certificate attribute deviates, it is marked as non-complaint and notified to users. Users can request for a new certificate (in-line to organization standards) to Certificate Authority.

Before you Begin

Following are the prerequisites for configuring a CA based **Policy** in **CERT+**:

- Certificate Group(s) must be available to map the **Policy** to them.
- CA accounts (settings) must be available to which the policy is going to be created.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Key Algorithm, Encryption Type must be available under the CA accounts.
- AppViewX permission required (**Accounts > Roles** - *Click here to check Accounts management)*

Access the following

- **CERT+ > Policy > View Policy** - To view the policy.
- **CERT+ > Policy > Add / Modify** - To create/ modify the policy.

- Configuring Policy Details
- Configuring a CA Policy for Amazon CA
- Configuring a CA Policy for Amazon Private CA
- Configuring a CA Policy for Digicert CA
- Configuring a CA Policy for Digicert One CA
- Configuring a CA Policy for EJBCA CA
- Configuring a CA Policy for Entrust CA
- Configuring a CA Policy for Entrust MPKI CA
- Configuring a CA Policy for Futurex
- Configuring a CA Policy for GlobalSign Atlas CA
- Configuring a CA Policy for GlobalSign CA
- Configuring a CA Policy for GlobalSign MSSL CA
- Configuring a CA Policy for GoDaddy CA
- Configuring a CA Policy for Google CA
- Configuring a CA Policy for HashiCorp Vault CA
- Configuring a CA Policy for HydrantID CA
- Configuring a CA Policy for IDnomic CA
- Configuring a CA Policy for Let's Encrypt CA
- Configuring a CA Policy for Microsoft Enterprise CA
- Configuring a CA Policy for Microsoft Standalone CA
- Configuring a CA Policy for Nexus CA
- Configuring a CA Policy for OpenTrust CA
- Configuring a CA Policy for Sectigo CA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Configuring a CA Policy for Symantec CA
- Configuring a CA Policy for Trustwave CA

Configuring Policy Details

1. Go to (**Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.

   Note: CERT+ is packaged with the following: default policies **Default** and **Certificate-Gateway**.

2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Enter the **Policy Details**.

Field description for Policy Details

Fields	Description
***Policy name**	Enter a unique name for the CA policy. • Only the following special characters are considered valid: **.**, **-**, and _. • The policy name cannot start with a special character (including the valid ones).
Description	Enter a description of the policy.
***Policy Enforcement Type**	Select **Strict** (default) or **Suggestive.** • **Strict** - Enforces standards defined in the policy where a user cannot modify any parameters. • **Suggestive** - Suggests policy parameters. A user can modify to the suggested values if required.
Certificate Requests Need Approval	To enforce peer approval process for any certificate requests raised, turn on the **Certificate Requests Need Approval** toggle. All CLM actions, such as certificate creation/renewal/regeneration/reissue/revocation, will now be executed after due approval is received. Peer approval for requests is defined in the approval workflow.
Enable Access to Private Key	When enabled, allows the user to download private keys from the holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Enable certificate push-bind access for a read-only user	Enabling this feature will allow a user from a read-only user group to perform certificate push, bind, and rollback operations from the holistic view.
Validate issuer and root certificate for compliance	Enabling this option will validate if the issuer and root of a certificate are also compliant with the standards defined in the policy.
Email Address mandatory for Client Certificate	Enabling this option will set the email address as mandatory during client certificate enrollment.
Enable Public Key Validation during CSR Upload?	To validate the public key included in the CSR uploaded for certificate enrollment, renewal, regenerate, or reissuance, turn on the **Enable Public Key Validation during CSR Upload?** toggle.
**: Mandatory fields*	

Note: You can configure the **Policy Details** section based on your organization's standards.

4. Under the **Group selection** section, select one or more groups to map to the policy.
5. Under the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

Configuring a CA Policy for Amazon CA

1. Go to (**Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** pane in the left, select **Amazon** .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for Amazon CA Details

Fields	Description
***CA Accounts**	The Amazon CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
**: Mandatory fields*	

5. From the **CA Accounts** dropdown list., select the required CA account.
6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. Enter the **Certificate Parameters**.

Field description for certificate parameters

Fields	Description
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

10. Click the **Save CA Details** button to save the configuration. A green tick mark will be displayed in the **Certificate Authority** pane against the **Amazon** option to indicate that the details are successfully stored.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click the **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a CA Policy for Amazon Private CA

Prerequisites:

- You must configure the CA setting with Amazon Private CA credentials.
- You must have validated and fetched the Amazon Intermediate CAs along with the issuer region details in the CA settings page.

1. Go to (**Menu)** > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Amazon Private CA**.
   The **CA Details** section is updated to display fields relevant to Amazon Private CA.
5. Enter the policy details for Amazon Private CA.

Field description to create CA policy for Amazon Private CA

Field	Description
***CA Accounts**	From the dropdown list, select the certificate authority account.
***Issuer Region**	From the dropdown list, select the issuer region.
***Issuer Name**	From the dropdown list, select the issuer name.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
***Bit Length - Key Type**	All the key types are listed with their corresponding bit length. You can select one or more than one bit length - key type pair from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>The discovered certificate's key type and bit length will be compared against the selected bit length - key type(s) to to check for compliance with the policy.

The selected bit length - key type(s) is enforced while performing any certificate request operations such as new, renew, regenerate. Amazon Private CA supports the following bit type and length:

<table>
<tr><th>Type</th><th>Length</th></tr>
<tr><td>RSA</td><td>2048

4096</td></tr>
<tr><td>EC</td><td>prime256v1 sec384r1</td></tr>
</table>
</td></tr>
<tr><td>*Hash Function</td><td>From the dropdown list, select one or more than one supported Hash Function. The supported hash functions are:
• SHA256
• SHA384
• SHA512</td></tr>
<tr><td>*Signature Algorithm</td><td>From the dropdown list, select the required signatire algorithm.

Note: The issuer will print the issuer algorithm that the users select from the Signature Algorithm in this field.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

6. Enter the **Certificate parameters** values.

Field description for certificate parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforcedat the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

7. Click **Save CA Details**.
   A green tick mark is displayed in the **Certificate Authority** pane against **Amazon Private CA** to indicate that the details are successfully stored.
8. From the **Group selection**, select one or more groups to map to the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

   Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

10. Click **Create Policy**.

    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Digicert CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.

   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.

   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **DigiCert**.

   The **CA Details** section is updated to display fields relevant to DigiCert.
5. Enter the policy details for DigiCert.

Field description for CA details

Fields	Description
***CA Account**	From the dropdown list, select an existing CA account for which this policy is to be created.
***Division**	Select the division from the dropdown list.
***Certificate Type**	Certificate types corresponding to the selected CA account are listed. Select one (or) more certificate types from the list to create the policy.
***Validity**	Enter a validity period for the certificate. The available options are: **Days** - You can enter more than one validity period in days, to choose one in certificate enrolment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Month - You can enter more than one validity period in Months, to choose one in certificate enrolment. **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment. **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment.
**: Mandatory fields*	

6. In the **Vendor Specific Details** section, select/enter the details as listed in the table

Field description for Vendor Specific Details

Fields	Description
***Server Type**	Select the server type from the dropdown list.
**: Mandatory fields*	

7. Click **Add**.
   The CA details are added to the table below the **Add** button and a confirmation message is displayed.

Note: You can use the **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

8. Select the **Bit Length -Key Type**, **ECDSA curve**, and the **Hash Function**.
9. Based on your organization's policies and standards, enter values for the **Certificate Parameters**.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), - (hyphen), . (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Digicert** to indicate that the details are successfully stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

11. From the **Group selection** section, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message displays.

Configuring a CA Policy for Digicert One CA

DigiCert One CA allows creation of certificate profiles using certain generic template ids which are eventually used during enrollment.

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **DigiCert One**.
   The **CA Details** section is updated to display fields relevant to DigiCert.
5. Enter the policy details for DigiCert One.

Field description for CA details

Fields	Description
***CA Accounts**	From the dropdown list, select an existing CA account for which this policy is to be created.
***Certificate Profiles**	From the dropdown list, select a certificate profiles.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Certificate profiles are created in the DigiCert One instance and provide you with the list of fields that are mandatory for certificate issuance and also other configured settings that have static values or allow multiple values. Values in the dropdown lists for the subsequent fields will be populated based on what is specified in the selected certificate profile.
***Validity**	Using the **Days**, **Months**, and **Years** dropdown lists, select a validity period for the certificate. **Days**: You can enter more than one validity period in days, to choose one in certificate enrolment. **Months** - You can enter more than one validity period in Months, to choose one in certificate enrolment. **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment. **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment. These dropdown lists are populated according to the certificate profile selected.
***Bit Length - Key Type**	From the ***Bit Length - Key Type** dropdown list, select the required bit length- key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected bit length- key type pair(s) to check for compliance with the policy. The selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **Enroll**, **Renew**, **Regenerate**.
***Hash Function**	From the ***Hash Function** dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	selected hash function(s) is enforced while performing any certificate request operations such as **Enroll**, **Renew**, **Regenerate**.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are added to the table below the **Add** button and a confirmation message is displayed.

> **Note:** You can use the **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

7. Based on your organization's policies and standards, enter values for the **Certificate Parameters**.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
Allowed Domain Names	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)
**: Mandatory fields*	

8. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** list against **Digicert One** to indicate that the details are successfully stored.
9. From the **Group selection** section, select one or more groups to map to the policy.
10. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

11. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a CA Policy for EJBCA CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **EJBCA**.
   The **CA Details** section is updated to display fields relevant to EJBCA.
5. In the **Vendor Specific Details** section, select/enter the details as listed in the table.

   Field descriptions for the vendor-specific details

Fields	Description
End entity user name	Enter the name of the end entity user.
***End entity Profile name**	Enter the name of the end entity profile.
***Issuer Common Name**	Enter the common user name.
***Certificate Profile Name**	Enter a certificate profile name.
**: Mandatory fields*	

6. Click **Add** .
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), - (hyphen), . (period)
*: Mandatory fields	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **EJBCA** to indicate the details are successfully stored.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Entrust CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Entrust**.
   The **CA Details** section is updated to display fields relevant to Entrust.
5. Enter the CA details for Entrust.

Field Description for CA Details

Fields	Description
***CA Accounts**	The Entrust CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The **Certificate Types** corresponding to the selected CA account are listed. Select one (or) more certificate types from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. In the **Vendor Specific Details** section, select/enter the details as listed in the table:

Fields	Description
Additional Emails	Enter the valid email address in the field.

7. Click **Add**.
   The CA details are saved to the table and the confirmation message displays.

   You can use the **Edit** option in the table to modify the configuration and **the Remove** option to delete the configuration.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.

10. Enter the **Certificate parameters to be Compared or Enforced**.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Use this toggle button to restrict the creation of wild card certificates using the policy.
Disable CT Logs	For Entrust CA, AppViewX lets you disable sending certificate data to the Certificate Transparency logs everytime a certificate is enrolled, renewed, regenerated, and/or reissued. To do this: • At the time of configuring the Entrust CA policy , turn on the **Disable CT Logs** button. Now, every time this Entrust policy is used to enroll/renew/ regenerate/reissue a certificate, its CT logs will not be generated and the contents of the certificate, including host names, will not be publicly visible.
Host Name	Enter the host name. The host name cannot start and end with a **.** (period)
Allowed Domain Names	Enter from the list of whitelisted domain names. To add multiple domain names, press **Enter** after adding each domain name.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

11. Click **Save CA Details** to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Entrust** option to indicate that the details are successfully stored.
12. From the **Group selection**, select one or more groups to map to the policy.
13. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the **Job Scheduler**.

14. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a CA Policy for Entrust MPKI CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Entrust MPKI**.
   The **CA Details** section is updated to display fields relevant to Amazon Private CA.
5. Enter the policy details for Entrust MPKI.

Field description for CA details

Fields	Description
***CA Accounts**	Select a CA account from the list to create the policy. The selected CA account will be listed in the **CA Accounts** table.
***Bit Length - Key Type**	From the dropdown list, select one (or more than one), bit length-key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Enter the **Certificate parameters** values.

Field description for certificate parameters

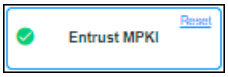
Fields	Description
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** pane against **Entrust MPKI** to indicate that the details are successfully stored.



8. From the **Group selection**, select one or more groups to map to the policy.
9. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

10. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Futurex

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy : Create** page is displayed.
3. Enter/Select the **Policy Details**.
   These details define the rules and templates for a certificate policy to ensure that certificate attributes are in compliance with the organization.

Field description for Policy Details

Fields	Description
***Policy name**	Enter a unique name for the CA policy. **Constraints**: • Only the following special characters are considered valid: **.**, **-**, and _. • The policy name cannot start with a special character (including the valid ones).
Description	Enter additional details related to the rules and guidelines enforced by the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Policy Enforcement Type	The policy enforcement type defines whether users can modify the policy parameters. Depending on your requirement, select one from the following values: • **Strict**: This selection will enforce the standards defined in the policy, not allowing users to modify any parameters. • **Suggestive**: This selection will suggest policy parameters, allowing the user to modify the suggested values as required.
Certificate Requests Need Approval	To enforce peer approval process for any certificate requests raised, turn on the **Certificate Requests Need Approval** toggle. All CLM actions, such as certificate creation/renewal/regeneration/reissue/revocation, will now be executed after due approval is received. Peer approval for requests is defined in the approval workflow.
Enable Access to Private Key	To allow the user to download private keys from the holistic view and the certificate inventory, turn on the **Enable Access to Private Key** toggle..
Enable certificate push-bind access for a read-only user	To allow users with only read-only access to perform the certificate push, bind, and rollback operations from the holistic view, turn on the **Enable certificate push-bind access for a read-only user** toggle.
Validate issuer and root certificate for compliance?	To validate the issuer and root of a certificate for compliance with the policy standards, enable the **Validate issuer and root certificate for compliance?** toggle.
Email Address mandatory for Client Certificate	At the time of client certificate enrollment, to set the email address field as mandatory, turn on the **Email Address mandatory for Client Certificate** toggle.
Enable Public Key Validation during CSR Upload?	To validate the public key included in the CSR uploaded for certificate enrollment, renewal, regenerate, or reissuance, turn on the **Enable Public Key Validation during CSR Upload?** toggle.
**: Mandatory fields*	

4. In the **CA Details** section:

   a. From the **Certificate Authority** list on the left, select **Futurex**.
   The section is updated to display the fields required to configure a Futurex policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

b. Enter/Select the CA details.

Field description for CA Details

Fields	Description
***CA Accounts**	From the dropdown list, select the CA account names of the CA settings that will be mapped to this policy.
***Issuance Policy**	From the dropdown list, select one from the list of issuance policies retrieved for the CA account name selected above. The issuance policy selected defines the set of rules and conditions under which certificates can be issued using this policy. This may include constraints like key length, usage, subject naming, and validity period.
***Root CA**	From the dropdown list, select the root CA for this certificate. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Validity**	Using the **Days**, **Months**, and **Years** dropdown lists, select a validity period for the certificate. **Days**: You can enter more than one validity period in days, to choose one in certificate enrolment. **Months**: You can enter more than one validity period in Months, to choose one in certificate enrolment. **Year**: You can enter more than one validity period in Year, to choose one in certificate enrolment.
***Bit Length - Key Type**	From the ***Bit Length - Key Type** dropdown list, select the required bit length- key type pair(s). The discovered certificates' key type and bit length will be compared against the selected bit length- key type pair(s) to check for compliance with the policy. The selected bit length- key type pair(s) is enforced while performing any certificate request operations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificates' key hash algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is/are enforced while performing any certificate request operations.
**: Mandatory fields*	

c. Click **Add**.
The CA details are added to the table below the **Add** button and a confirmation message is displayed.

Note: You can use the **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

d. Enter/Select the **Certificate Parameters** for the policy.
The parameters of a discovered certificate will be compared the values entered in this section to assess its compliance with this policy.

Field description for CA Details

Fields	Description
Restrict Wild Card Certificate	To restrict the creation of wild card certificates using this policy, turn on the **Restrict Wild Card Certificate** toggle. A **wildcard certificate** is a type of SSL/TLS certificate that secures **a domain and all its subdomains** using a single certificate. This could possess a security risk considering that if this certificate is compromised, all its subdomains become vulnerable.
Host Name	Enter a host name that will be used to identify the domain secured by the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Constraints: • The host name cannot start and end with a **.** (period). • If a host name is not specified here, the user is allowed to enter a host name of their choice at the time for creating certificate requests for CLM actions.
Allowed Domain Names	Enter the domain names that must be whitelisted for this policy. Multiple domain names can entered, separated by the **Enter** key. If this field is left blank, by default, all domains will be whitelisted for the CLM actions that use this policy.
Blocked Domain Names	Enter the domain names that must be blacklisted for this policy. Multiple domain names can entered, separated by the **Enter** key. If this field is left blank, by default, all domains will be blacklisted for the CLM actions that use this policy.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificates' **Subject Organization** is checked for compliance with this value. The organization name is enforced while performing any certificate request operations.
Organization Unit	Enter the name of the business unit of the organization.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certfiicates' **Subject Organization Unit** is checked for compliance with this value. The organization unit name is enforced while performing any certificate request operations.
Locality	Enter the organization's locality name. The discovered certfiicates' **Locality** is checked for compliance with this value. The locality name is enforced while performing any certificate request operations.
State	Enter the name of the state in which the organization is located. The discovered certfiicates' **State** is checked for compliance with this value. The state name is enforced while performing any certificate request operations.
Country code	Enter the organization's country code. The discovered certfiicates' **Country Code** is checked for compliance with this value. The state name is enforced while performing any certificate request operations.
Email	Enter the organization unit's official email address. The email address specified for the discovered certfiicates' is checked for compliance with this value. The value is enforced while performing any certificate request operations.
Subject Alternative Name	Enter the subject alternative name (SAN) applicable for this policy. The SAN helps enforce additional domains for which a certificate can be requested. It is enforced at the time of performing certificate request operations. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

e. Click **Save CA Details**.
A green tick mark is displayed in the **Certificate Authority** list against **Futurex** to indicate that the details are successfully stored.

5. Under the **Group selection** section, select one or more groups to map to the policy.
6. Under the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

7. Click **Create Policy**.
The policy is created and a confirmation message is displayed.

Configuring a CA Policy for GlobalSign Atlas CA

Before You Begin: The prerequisites for configuring the policy are as follows:

- Certificate group(s) must be available to map the policy to them.
- CA accounts (settings) must be available to which the policy is going to be created.
- AppViewX permissionis required (**Accounts** > **Roles** - Click here to check Accounts Management).

To configure policy for GlobalSign Atlas CA:

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
The **CA Policy** page is displayed.

   CERT+ is packaged with the following default policies: **Default** and **Certificate-Gateway**.

> **Note:** The **Default** CA Policy will have the **GlobalSign Atlas CA** details.

2. Click **+ Create** to configure GlobalSign Atlas custom policy.
The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Policy Details**
- **Group Selection**
- **Compliance Check**

4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **GlobalSign Atlas**.
   The **CA Details** section is updated to display fields relevant to GlobalSign Atlas.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The GlobalSign Atlas CA accounts configured in the CA settings screen are listed here. Select a CA account from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
***Bit Length - Key Type**	From the dropdown list, select one (or more than one), bit length- key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

The updated fields for the CA are displayed on the right.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Add**.
   The CA details are saved in the table and the confirmation message is displayed.

   You can use the **Edit** (pencil)option in the table to modify the configuration and the **Remove** (bin) option to delete the configuration.

7. Enter the **Certificate parameters** values.

Field description for certificate parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

8. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** pane against **GlobalSign MSSL** to indicate that the details are successfully stored.
9. From the **Group selection**, select one or more groups to map to the policy.
10. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

11. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for GlobalSign CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **EJBCA**.
   The **CA Details** section is updated to display fields relevant to EJBCA.
5. In the **Vendor Specific Details** section, select/enter the details as listed in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for vendor specific details

Fields	Description
***Incorporating Agency Reg. No**	Enter the agency registration number.
***Designation**	Enter the designation.
***Business Category**	Select the business category from the dropdown list.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the white-listed domain names.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period) .
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **GlobalSign** to indicate that the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for GlobalSign MSSL CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** to configure a GlobalSign MSSL based policy.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **GlobalSign MSSL**.
   The **CA Details** section is updated to display fields relevant to GlobalSign MSSL.
5. Enter the CA details.

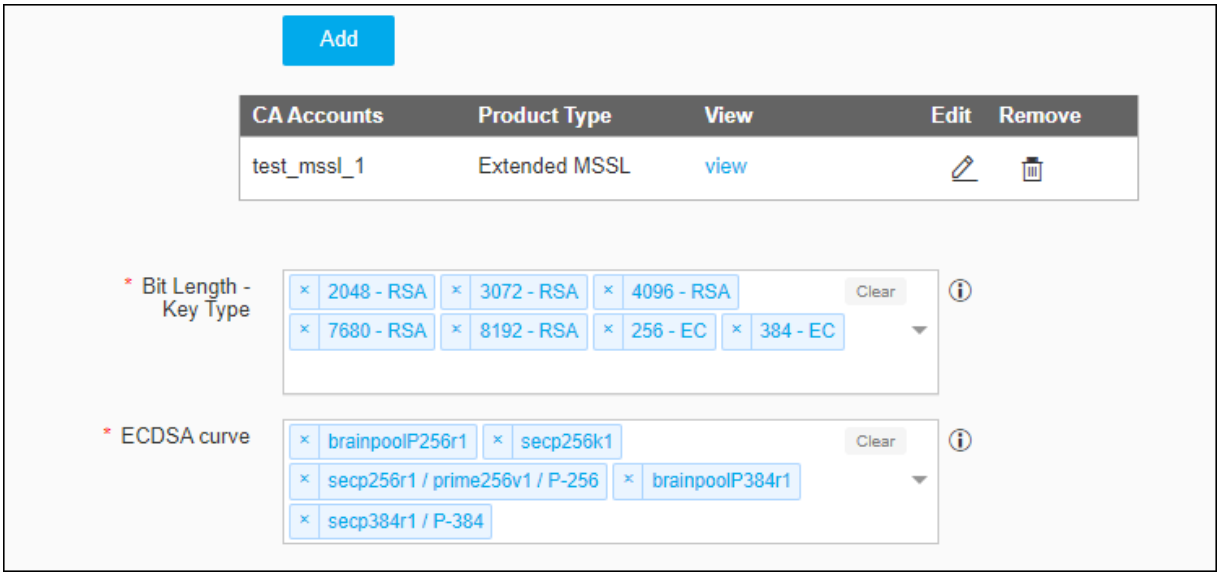
Field description for CA details

Fields	Description
***CA Accounts**	The GlobalSign MSSL CA accounts configured on the CA settings screen are listed. Select a CA account from the list to create the policy.
* **Product Type**	All Managed SSL Product Types require that the Organization's information and at least one Domain be registered in the Managed SSL account prior to ordering.
***Signature Algorithm**	Select the signature algorithm from the dropdown list list.
* **MSSL Profile Allowed Domain Name**	Select the **MSSL Profile Allowed Domain Name** from the dropdown list list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.



   You can use **Edit** option in the table to modify the configuration and the **Remove** option to delete the configuration.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **GlobalSign MSSL** to indicate that the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for GoDaddy CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **GoDaddy**.
   The **CA Details** section is updated to display fields relevant to GoDaddy.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Account**	The GoDaddy CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	The **Certificate Types** corresponding to the selected CA account are listed. Select one (or) more **Certificate Type** from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
7. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
9. Enter the certificate parameters.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **GoDaddy** to indicate that the details are successfully stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Google CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy : Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Google**.
   The **CA Details** section is updated to display fields relevant to Google.
5. Enter the CA details.

Field description for CA details

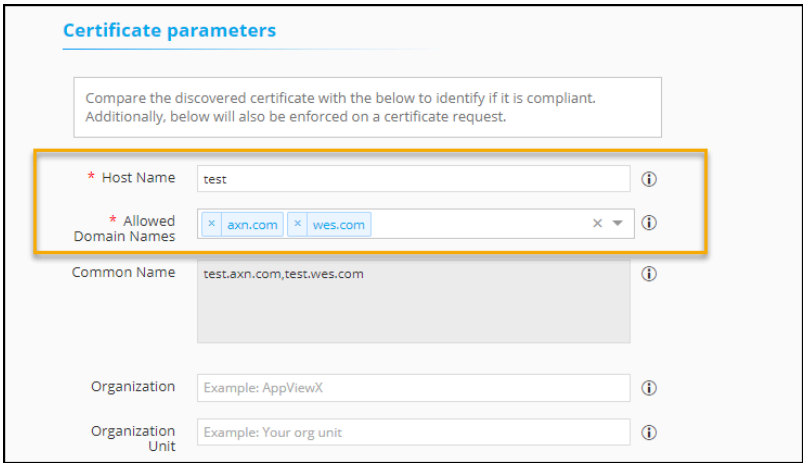
Fields	Description
***CA Accounts**	The Google CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Issuer Location**	The issuer locations corresponding to the selected CA account are listed. Select an issuer location from the list to create the policy.
***Issuer Name**	The issuer names corresponding to the selected CA account are listed. Select an issuer name from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
***Bit Length - Key Type**	From the dropdown list, select one (or more than one), bit length-key type pair(s). The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
***Hash Function**	From the dropdown list, select one (or more) hash functions. The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

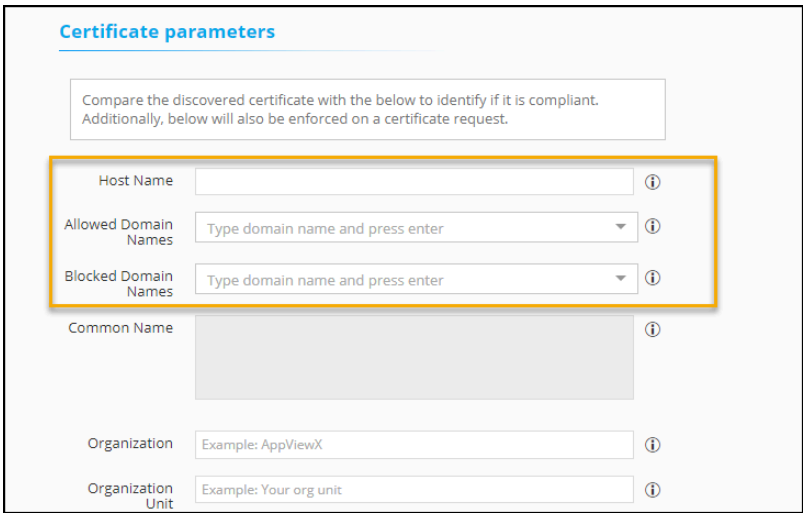
6. Enter the certificate parameters.

   For **Policy Enforcement Type** = **Strict**



   For **Policy Enforcement Type** = **Suggestive**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Field description for certificate Parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Hostname	This text field is displayed if the **Policy Enforcement Type = Strict** or **Suggestive**. Enter the unique name or label for the host. The field is **mandatory** only when the **Policy Enforcement Type = Strict**. **Note:** The hostname should not start or end with a dot.
Allowed Domain Name	This text field is displayed if the **Policy Enforcement Type = Strict** or **Suggestive**. The field is **mandatory** only when the **Policy Enforcement Type = Strict**. Enter the valid domain name (two parts separated by a dot, such as example.com).
Blocked Domain Name	This text field is displayed only if the **Policy Enforcement Type = Suggestive** Enter the domain names (two parts separated by a dot, such as example.com) that need to be blocked

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	You can provide the organization's name. The discovered certificate's **Subject Organization** will be compared against the organization provided in the policy to identify if they are complaints. The organization is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	You can provide an organization unit. The discovered certificate's **Subject Organization Unit** will be compared against the organization unit provided in the policy to identify if they are Complaint. Organization Unit is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	You can provide a locality. The discovered certificate's **Locality** will be compared against the locality provided in the policy to identify if they are complaints. The locality is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	You can provide state. The discovered certificate's **State** will be compared against the state provided in the policy to identify if they are complaints. The state is enforced

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	You can provide a country code. The discovered certificate's **Country code** will be compared against the country code provided in the policy to identify if they are complaints. Country code is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	You can provide an organization unit mail address. The discovered certificate's **mail address** will be compared against the email address provided in the policy to identify if they are Complaint. Mail address is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	You can provide the subject alternative name (SAN) It helps enforce additional domains for which a certificate can be requested. Subject Alternative Name is enforced while performing certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use Asterisk (*) for the host part of the FQDN to enforce the domain. For example, *.domain.com will only allow users to request certificates with domain domain.com. Allowed Special Characters: Asterisk (*), Hyphen (-), Period (.), At (@).
**: Mandatory fields*	

You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Accounts	Issuer Location	Issuer Name	validity	Edit	Remove
Google CA	us-east1	AppViewX-Enterprise-Pvt-Root-CA-1023	view		
Google CA 1	us-central1	AppViewX-Enterprise-Pvt-Root-CA-1029	view		

7. Click **Save CA Details** to save the configuration.
   A green tick mark is displayed in the **Certificate Authority** pane against **Google** to indicate the details are successfully stored.
8. From the **Group selection**, select one or more groups to map to the policy.
9. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

10. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for HashiCorp Vault CA

Before You Begin

- Certificate Group(s) must be available to map the Policy to them.
- CA accounts (settings) must be available to which the policy is going to be created.
- Key Algorithm, Encryption Type must be available under the CA accounts.
- AppViewX permission required (Accounts > Roles - Click here to check Accounts management).

To configure a Hashicorp Vault CA policy:

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed with a list of policies and their associated groups.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: A **Default** policy will always be present in the list. Most of the roles are mapped to this policy. This policy can be used for any of the configured CAs.

2. To create a custom policy, click **+Create** from the top-right corner of the **CA Policy** page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **HashicorpVault**.
   The **CA Details** section is updated to display fields relevant to HashicorpVault.
5. Enter the CA details.

Field Description for CA Details

Fields	Description
***CA Accounts**	Select a CA account from the list to create the policy.
***Secret Engine**	The single-select dropdown contains all the secret engines associated with the account. In a secret engine, a role describes an identity with a set of permissions, groups, or policies you want to attach to a user of the secret engine. User identity is often mapped to a specific role. Hence, a single secret engine needs to be selected to populate role (below) specific to it.
***Role**	The dropdown list contains all the roles mapped to the secret engine.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

CA Settings	Secret Engine	Role	View	Edit	Remove
APPROLE-DEMO	pki_int	Server-Certificate	View		
APPROLE-DEMO	pki_int	certificate-role	View		

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Multiple values can be configured based on the available CA settings and secret engines with different bit length - key type and hash function. The supported values include:

- **Key Type**: RSA, EC
- **Bit Length:**
  - *RSA key type*: 2048 (default), 3072, or 4096
  - *EC key type*: 224, 256 (default), 384, or 521
- **Hash Function**: SHA-256, SHA-384, SHA-512

The CA Details table has options to **View**, **Edit**, and **Delete**.

a. To view the CA details, click the **View** link in the **View** column. The CA account details are displayed in a pop-up window with the **Bit Length - Key Type** and **Hash Function.**
b. To update the CA details, click the edit icon in the **Edit** column.
c. To delete the CA details, click the delete icon.

7. Enter the certificate parameters.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

8. Click **Save CA Details**.
   A green tick mark is displayed in the **Certificate Authority** pane against the **Hashicorp Vault** option to indicate that the details are successfully saved.
9. In the **Group Selection**, select one or more groups to map to the policy. Refer to the **Certificate Group** section to add/update groups.
10. Under the **Compliance Check** section, enable the **Perform Compliance Check** option to perform an immediate compliance check.
11. Click **Create Policy** button.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for HydrantID CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **HydrantID**.
   The **CA Details** section is updated to display fields relevant to HydrantID.
5. Enter the CA details.

Field Description for CA Details

Fields	Description
***CA Accounts**	The HydrantID CA accounts configured in the CA settings screen are listed here. Select a CA account from the list to create the policy.
***HydrantID Policy**	Policies associated with the account will be displayed here. Select a policy from the dropdown (single select).
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select the required encryption algorithm (key type) and the corresponding key size (bit length) for key generation
   For discovery, the discovered certificate's key type and bit length will be compared against the selected bit length- key type pair(s) to check for compliance with the policy. The selected bit length-key type pair(s) is enforced while performing any certificate request operations such as **Enroll**, **Renew**, **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. When **EC** is the selected key type, from the ***ECDSA curve** dropdown list, select the elliptic curve that will be used for key generation.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
10. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

11. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against the **HydrantID** CA option to indicate that the details are successfully stored.
12. From the **Group selection**, select one or more groups to map to the policy.
13. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

14. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for IDnomic CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed with a list of policies and their associated groups.

   Note: A **Default** policy will always be present in the list. Most of the roles are mapped to this policy. This policy can be used for any of the configured CAs.

2. To create a custom policy, click **+Create** from the top-right corner of the **CA Policy** page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Policy Details**
- **Group Selection**
- **Compliance Check**

4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **IDnomic**.
   The **CA Details** section is updated to display fields relevant to IDnomic.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The IDnomic CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Management Profile**OR ***Certificate Workflows**	If the selected CA Account is configured with a certificate profile then the field label is Certificate Management Profile and displays only certificate profiles. If configured with a registration authority (RA) the field label is Certificate Workflows and displays the certificate workflows. The Certificate Types corresponding to the selected CA account are listed. Select one (or) more Certificate Type from the list to create the policy.
***Validity**	Enter the validity period for the certificate. The available options are: • **Days** - You may enter more than one validity period in days, to choose one in certificate enrollment. • **Month** - You can enter more than one validity period in Months, to choose one in certificate enrollment. • **Year** - You can enter more than one validity period in Year, to choose one in certificate enrolment.
***Bit Length - Key Type**	All the Key Types are listed with corresponding Bit Length. You can select one (or) more than one Bit Length - Key Type(s) from the dropdown list. The discovered certificate's Key Type and Bit length will be compared against the selected Bit Length - Key Type(s) to identify if they are compliant with the policy. Selected Bit Length - Key Type(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Hash Function**	Supported Hash Function(s) are listed here. You can select one (or) more Hash Function(s) from the dropdown list. The discovered certificate's Key Hash Algorithm will be compared against the selected Hash Function(s) to identify if they are compliant with the policy. Selected Hash Function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed. You may use the **Edit** (pencil) option in the table to modify the configuration and the **Remove** (bin) option to delete the configuration.
7. Enter the certificate parameters.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Restrict users of the associated group policy from requesting Wildcard Certificates. Choosing this option will not allow Common Name or DNS starting with *.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

8. Click **Save CA Details**.
   A green tick mark is displayed in the **Certificate Authority** pane against the **IDnomic** option to indicate that the details are successfully saved.
9. In the **Group Selection**, select one or more groups to map to the policy. Refer to the **Certificate Group** section to add/update groups.
10. Under the **Compliance Check** section, enable the **Perform Compliance Check** option to perform an immediate compliance check.
11. Click **Create Policy** button.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Let's Encrypt CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **LetsEncrypt**.
   The **CA Details** section is updated to display fields relevant to LetsEncrypt.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Let's Encrypt CA accounts configured in CA settings are listed here. Select a CA account from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
Note: The asterisk (*) symbol indicates a mandatory field.	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **LetsEncrypt** to indicate that the details are successfully stored.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Microsoft Enterprise CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Microsoft Enterprise**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **CA Details** section is updated to display fields relevant to Microsoft Enterprise.

5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Microsoft Enterprise CA accounts configured in the CA settings are listed. Select a CA account from the list to create the policy.
***MS Template List**	The MS templates configured for the selected CA account are listed. Select MS template(s) from the list to associate with the policy.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Microsoft Enterprise** to indicate the details are successfully stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Microsoft Standalone CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Microsoft Standalone**.
   The **CA Details** section is updated to display fields relevant to Microsoft Standalone.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Microsoft Standalone CA accounts configured in the CA settings are listed. Select a CA account from the list to create the policy.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.

7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Microsoft Standalone** to indicate the details are successfully stored.
11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring a CA Policy for Nexus CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Nexus**.
   The **CA Details** section is updated to display fields relevant to Nexus.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Nexus CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate. You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Once the CA account and the validity fields are populated, a new section called **Vendor Specific Details** is enabled. Select the **Procedure** field from the dropdown list list and click **Add** to save the CA details to the table. You can also use the **Remove** option to delete the configuration.
   Select the details as follows:
   a. **Case 1 -** Select **Server** check box, the procedures listed in the **Procedures** dropdown will be - Mapped to servers and default procedures.
   b. **Case 2 -** Select **Client** check box, the procedures listed in the **Procedures** dropdown will be - mapped to client and default procedures.
   c. **Case 3 -** Select **Server** and **Client** check box, the procedures listed in the **Procedures** dropdown will be - mapped to server, client, and default procedures.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: The procedures displayed in the dropdown should have the **cert type** appended in the value. For example: - *Procedure name_Server/client/default/Code-Signing*.

7. Click **Add**. The CA details are saved to the table and the confirmation message displays.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. From the ***Hash Function** dropdown list, select one (or more) hash functions.
    The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
11. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com**

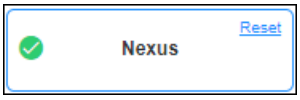
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

12. Click **Save CA Details** button to save the configuration.
    A green tick mark will be displayed in the **Certificate Authority** pane against **Nexus** to indicate that the details are successfully stored.



13. From the **Group selection**, select one or more groups to map to the policy.
14. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

15. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for OpenTrust CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **OpenTrust**.
   The **CA Details** section is updated to display fields relevant to OpenTrust.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Account**	The OpenTrust CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Management Profile**	Select the certificate management profile from the dropdown list.
***Zone**	Select the zone from the dropdown list.
**: Mandatory fields*	

6. Enter the **Profile Parameters**.

Field Description for profile parameters

Fields	Description
***Common Name**	Enter a common name for the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Organizational Unit	Enter the organizational unit.
Organization	Enter the name of the organization.
**: Mandatory fields*	

7. Click **Add** button.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use the **Remove** option to delete the configuration.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
9. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. From the ***Hash Function** dropdown list, select one (or more) hash functions.
    The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
11. Enter/Select the **Certificate parameters** values.

Field description for certificate parameters

Field	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

12. Click **Save CA Details** button to save the configuration.
    A green tick mark displays in the **Certificate Authority** pane against **OpenTrust** to indicate that the details are successfully stored.
13. From the **Group selection**, select one or more groups to map to the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

14. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

    Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

15. Click **Create Policy** to create a new policy.

    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Sectigo CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.

   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.

   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Sectigo**.

   The **CA Details** section is updated to display fields relevant to Sectigo.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Accounts**	The Sectigo CA accounts configured in the CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The certificate types corresponding to the selected CA account are listed. Select one (or) more certificate type(s) from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: ***(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

11. Click **Save CA Details** button to save the configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A green tick mark is displayed in the **Certificate Authority** pane against **Sectigo** to indicate that the details are successfully stored.

12. From the **Group selection**, select one or more groups to map to the policy.
13. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

14. Click **Create Policy** to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Symantec CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Symantec**.
   The **CA Details** section is updated to display fields relevant to Symantec.
5. Enter the CA details.

Field description for CA details

Fields	Description
***CA Account**	The Symantec CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The certificate types corresponding to the selected CA account are listed. Select one (or) more certificate type(s) from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. In the **Vendor Specific Details section**, select the server type from the dropdown list.
7. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
8. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
10. From the ***Hash Function** dropdown list, select one (or more) hash functions.
    The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, **Regenerate**.
11. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wildcard certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com** This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the * (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *(Asterisk), - (hyphen), . (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code. The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
**: Mandatory fields*	

12. Click **Save CA Details** button to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Symantec** to indicate that the details are successfully stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

13. From the **Group selection**, select one or more groups to map to the policy.
14. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

> **Note:** A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

15. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring a CA Policy for Trustwave CA

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **CA Policy**.
   The **CA Policy** page is displayed.
2. Click **+ Create** from the top-right corner of the page.
   The **CA Policy :: Create** page is displayed.
3. Refer the Configuring Policy Details section to configure the following:
   - **Policy Details**
   - **Group Selection**
   - **Compliance Check**
4. In the **CA Details** section, from the **Certificate Authority** list in the left, select **Trustwave**.
   The **CA Details** section is updated to display fields relevant to Trustwave.
5. Enter the CA details.

Field description for CA Details

Fields	Description
***CA Account**	The Trustwave CA accounts configured in CA settings screen are listed. Select a CA account from the list to create the policy.
***Certificate Type**	The certificate types corresponding to the selected CA account are listed. Select one (or) more certificate type(s) from the list to create the policy.
***Validity**	In the **Days**, **Month**, and **Year** dropdown lists, enter the validity period(s) for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	You can enter more than one validity period in days/months/years, and one can then be chosen from the entered values at the time of certificate enrollment.
**: Mandatory fields*	

6. Click **Add**.
   The CA details are saved to the table and the confirmation message is displayed.

   You can use **the Edit** option in the table to modify the configuration and **Remove** option to delete the configuration.
7. From the ***Bit Length - Key Type** dropdown list, select one (or more than one), bit length- key type pair(s).
   The discovered certificate's Key Type and Bit length will be compared against the selected B bit length- key type pair(s) to check for compliance with the policy. The Selected bit length- key type pair(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
8. From the ***Hash Function** dropdown list, select one (or more) hash functions.
   The discovered certificate's Key Hash Algorithm will be compared against the selected hash function to check for compliance with the policy. The selected hash function(s) is enforced while performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
9. Enter the **Certificate parameters** values.

Field description for certificate parameters

Fields	Description
Restrict Wild Card Certificate	Slide toggle switch to the ON position to restrict the creation of wild card certificates using the policy.
Host name	Enter the host name. The host name cannot start and end with a **.** (period)
***Allowed Domain Names**	Enter only the whitelisted domain names. Press enter after adding the domain name. Multiple domain names can be added.
Common Name	Enter the common name. For example, ***.domain.com**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	This enforces domains for which a certificate can be requested. The common name is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period).
Organization	Enter the organization name. The discovered certificate's subject organization will be compared against the organization provided in the policy to check for compliance. The organization is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Organization Unit	Enter the organization unit. The discovered certificate's Subject Organization Unit will be compared against the organization unit provided in the policy to check for compliance. Organization Unit is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Locality	Enter the locality name. The discovered certificate's locality will be compared against locality provided in the policy to check for compliance. The locality is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
State	Enter the state. The discovered certificate's state will be compared against the state provided in the policy to check for compliance. The state is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Country code	Enter the country code.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The discovered certificate's country code will be compared against the country code provided in the policy to check for compliance. Country code is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Email	Enter the email address of the organization unit. The discovered certificate's email address will be compared against the email address provided in the policy to check for compliance. The email address is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**.
Subject Alternative Name	Enter the subject alternative name (SAN). It helps enforce additional domains for which a certificate can be requested. The SAN is enforced at the time of performing any certificate request operations such as **New**, **Renew**, and **Regenerate**. **Note:** Use the ***** (asterisk) for the host part of the FQDN to enforce the domain. For example, ***.domain.com** will only allow users to request certificates with domain.com. Allowed special characters: *****(Asterisk), **-** (hyphen), **.** (period) .
**: Mandatory fields*	

10. Click **Save CA Details** button to save the configuration.
    A green tick mark is displayed in the **Certificate Authority** pane against **Trustwave** to indicate that the details are successfully stored.

11. From the **Group selection**, select one or more groups to map to the policy.
12. From the **Compliance Check** section, to perform an immediate compliance check, enable **Perform Compliance check**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: A scheduled compliance check will run periodically based on the settings defined in the job scheduler.

13. Click **Create Policy** button to create a new policy.
    The policy is created and a confirmation message is displayed.

Configuring Certificate Groups

Prerequisites for Configuring Groups

Know the following before starting the **Certificate Groups** configuration:

- **Certificate Groups** are used to categorize the certificates according to various **business units.**
- In some organizations, **Certificate Groups** are also used to assign access permissions. Only privileged users (inherits from Resource > User Group) can view the respective **Certificate Groups**.
- Users should be assigned to a **Role** (inherited from Role > User Group) that has access to perform the below actions:
  - View a group
  - Assign a group
  - Unassign a group
- With these actions, users can assign a group during **Certificate Discovery** to avoid movement of certificates post-discovery.
- Along with the view, assign, and unassign options, administrators should be assigned to a **Role** that has access for additional actions:
  - Create/ modify a group
  - Delete a group
  - Edit Default group

Creating a Group

Assign the user to a user group that (inherits from resource and role) have access to certificate group.

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **Groups**.
   The Group inventory is displayed. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway.**
2. Click the **+ Create** button in the command bar to create a new group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter the **Group Details**.

Field descriptions for Group Details

Field	Description
***Select Group Hierarchy**	From the dropdown list, select the parent group to which the new group should be associated: • **Default** • **Certificate Gateway** • **Private CA Certificates** • **Public CA Certificates**
***Group Name**	Enter a unique name for the new group. **Constraints**: • Group name should not begin with a special character and/or a space. • Group name should not end with a space. • Valid special characters: **( )**, **.**, **-**, **/**, **+**, **&**, _
Display Name	Enter a unique name for the new group. You can use this display name to filter the group while configuring expiry alerts. **Constraints**: • Group name should not begin with a special character and/or a space. • Group name should not end with a space. • Valid special characters: **.**, **-**, _
Application ID	Enter the organization ID (if any) to associate with the new group.
Description	Enter the purpose of the certificate group.
**: Mandatory fields*	

4. Enter the **Other Details** for the new certificate group, based on the organization's requirement.

Field descriptions for the Other Details

Name	Description
First Name	First name of the point of contact
Last Name	Last name of the point of contact

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
Contact Name	Provide contact person to whom changes should be intimated
Line of Business Name	Provide the name of the business unit
Email	Provide contact mail address
Alternative Email(s)	Provide alternative contact mail address
Environment Name	Provide environment name
Phone Number	Provide a phone number for contact
Inventory Number	Enter the inventory number.
Cost Center/ Hierarchy	Enter the cost center code/ label.
Push Certificate Automatically	Select this checkbox to enable the auto push feature for this certificates that will be assigned to this group. **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function. The auto push feature is a mechanism that automatically pushes renewed/regenerated certificates to their target endpoints without any manual intervention. When this checkbox is selected, certificates assigned to this group will be pushed to their target endpoints as soon as they are renewed/ regenerated.
Select Application Connectors to Exclude from Cloning	From the dropdown list, select a status value to exclude the corresponding application connectors from cloning after certificate renewal, regeneration, and reissue.
Renew Automatically	To automatically renew certificates assigned to this group, turn on the **Renew Automatically** toggle.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
	Important: This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates).
***Start Renewing**	This field is displayed when **Renew Automatically** is enabled. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120**
Approval Required	This field is displayed when **Renew Automatically** is enabled. To ensure that the group inherited renewal configuration overwrites the certificate level renewal configuration (specified at the time of enrollment), select this checkbox.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time certificates belonging to this group are auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, all certificates in this group will inherit the setting. You can override it at the certificate level, unless group-level overrides are enforced.
Regenerate Automatically	To automatically regenerate certificates assigned to this group, turn on the **Regenerate Automatically** toggle.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
	Important: • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • When **Regenerate Automatically** is enabled, by default, the **Renew Automatically** feature is disabled. • To enforce AppViewX as the default CSR generation source everytime certificates in this group are regenerated, execute the following db script: `db.cert_metadata.insertOne ({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`
***Start Regenerating**	This field is displayed when **Regenerate Automatically** is enabled. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates.
Approval Required	This field is displayed when **Regenerate Automatically** is enabled. To ensure that the group inherited regeneration configuration overwrites the certificate level regeneration configuration (specified at the time of enrollment), select this checkbox.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time certificates belonging to this group are auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
	notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, all certificates in this group will inherit the setting. You can override it at the certificate level, unless group-level overrides are enforced.
Override	For a certificate, auto renewal/regeneration can be configured at the group level as well as at the certificate level at the time of certificate enrollment. To enforce group level auto renewal/regeneration settings across all certificates in the group, select the **Override** checkbox. Selecting this checkbox will override any changes made to the auto renewal/reconfiguration settings at the time of certificate enrollment.
***Associated Policy**	From the dropdown list, select the certificate policy that will be associated with this certificate group. This association helps enforce consistent standards for certificate issuance, renewal, and compliance across all certificates within the group.

5. Click **Create** button to create the group.
   Users can view the group only if it is associated with the **Resource** of their **User Group**. To associate the **Group** to a **Resource** click the **Update Group and Configure the Resources for User Access** button instead of **Create** button. This will create the group and navigates to **Resource**.
   The newly created **Group** is added to the Group inventory. Click the **Name** (Group name) to view the group details.

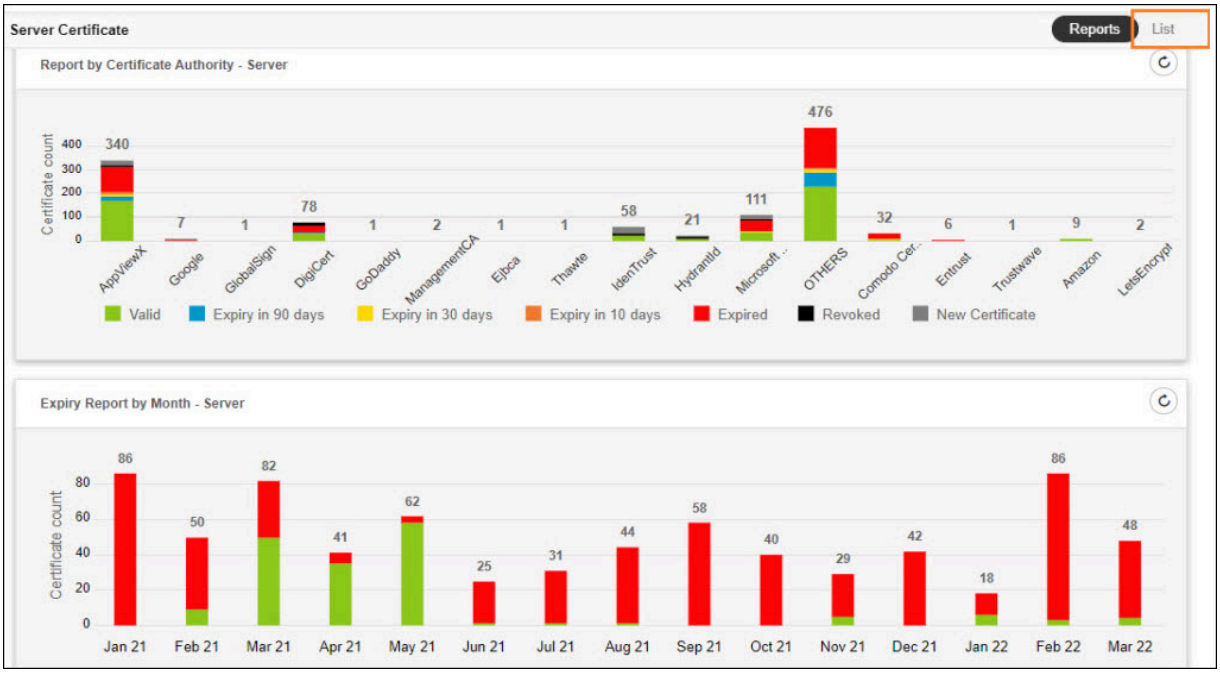
   Post certificate discovery, you can view the count of certificates (Server, Client, Device, and Code Signing) associated with this group.
6. Click the count in the Server Certificates column to view the certificates.

Assigning a Certificate to a Group

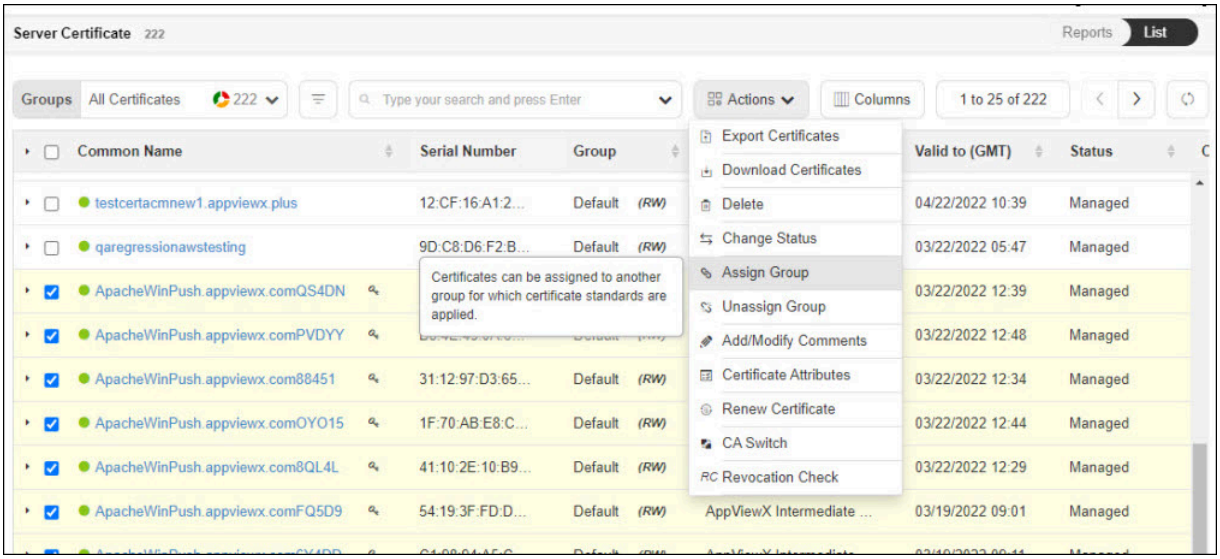
1. Go to (**Menu**) > **CERT+**.
   The **Server Certificate** Inventory is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click **List** from the upper right corner of the server certificate inventory screen.



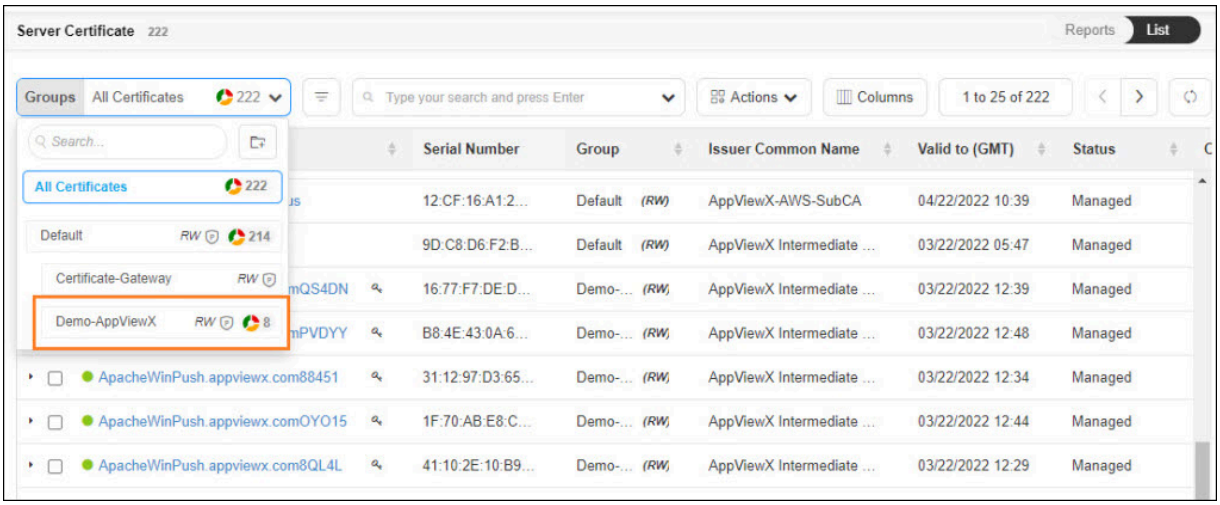
3. Select the check box against the certificate(s) you want to assign to a group.
4. Click the **Actions** dropdown list and select the **Assign Group** option from the dropdown list.



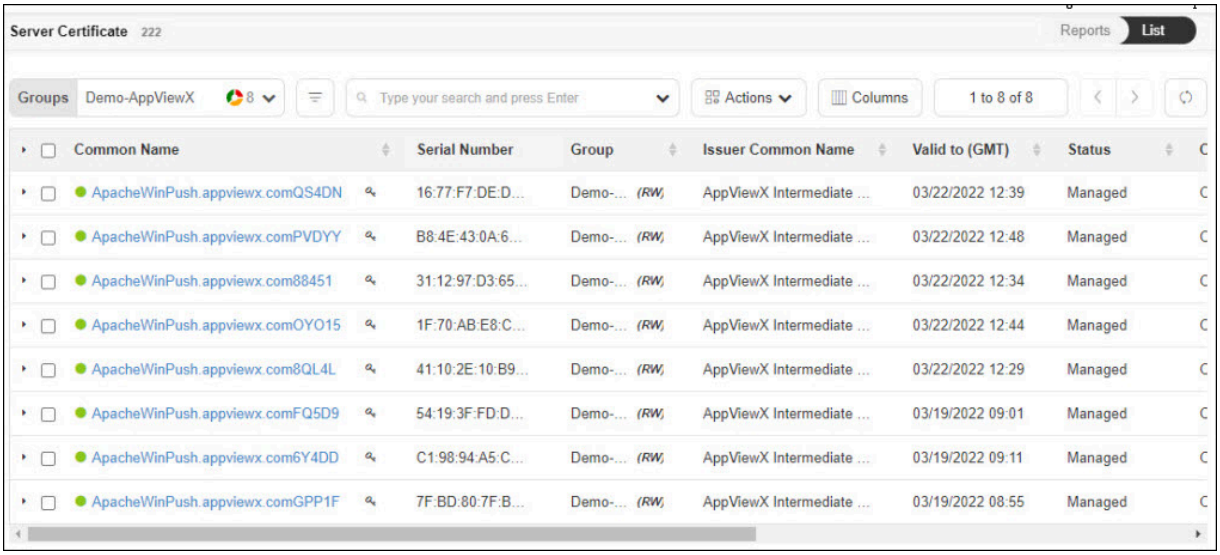
The **Assign to Group** pop-up is displayed.

5. Select **Group** from the list.
6. Click **Assign** to move the certificate(s) to the selected **Group.**
7. From the **Groups** dropdown list, select the required **Group** .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



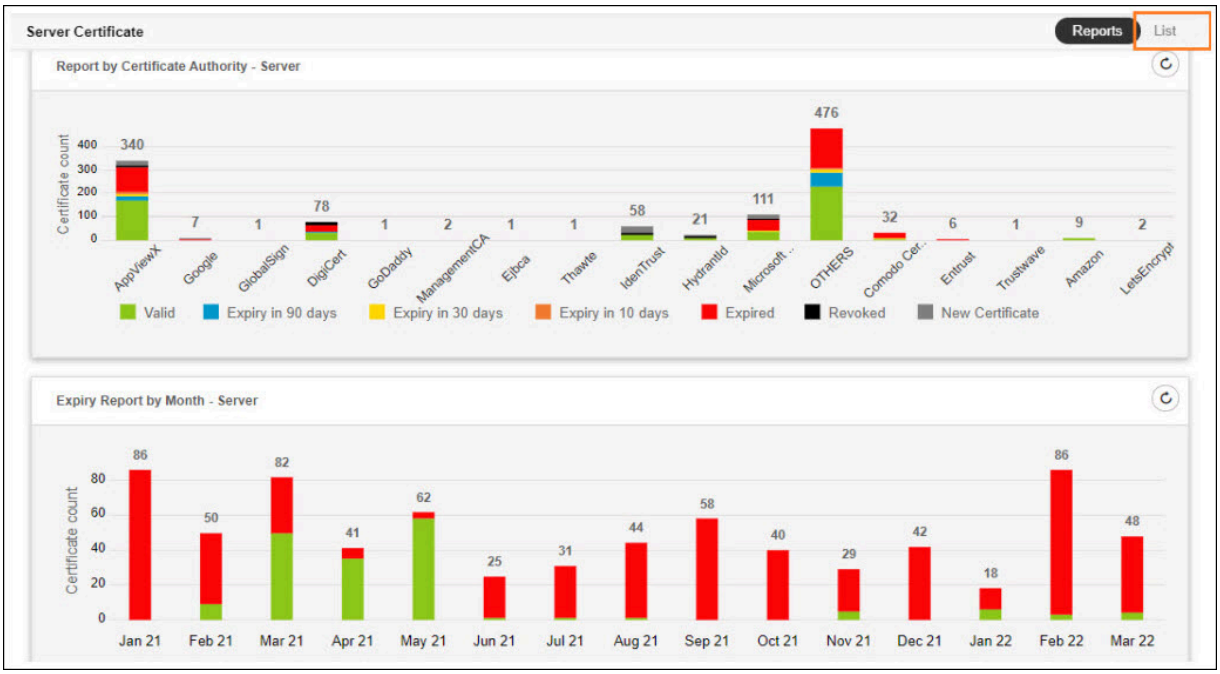
You can view the certificate(s) assigned to the **Group**.



Unassigning a Certificate from a Group

1. Go to (**Menu**) > **CERT+**.
   The **Server Certificate** Inventory is displayed.
2. Click **List** from the upper right corner of the server certificate inventory screen.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



3. From the **Groups** dropdown list, select the required **Group**.
4. Select the checkbox against the certificate you want to unassign from the group.
5. From the **Actions** dropdown list, select **Unassign Group** .
   The certificate is unassigned from your **Group** and automatically assigned to the **Default Group**.

What to do next?

A certificate should always assign to a **Group** to compliance with the **Policy**. Certificate unassigned from a group will automatically assign to **Default Group** and compliance against **Default Policy**.

Modifying a Group

Assign the user to a user group that (inherits from resource and role) have access to the certificate group

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **Groups**.
   The Group inventory is displayed. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway.**
2. Click the **Name** (Group name) to view the group details.
3. Modify required fields in the group and click the **Update** button. You can refer to the field descriptions explained in the Creating a Group section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Deleting a Group

1. Go to (**Menu**) > **CERT+** > **GROUPS & POLICIES** > **Groups**.
   The Group inventory is displayed. **CERT+** is packaged with default certificate groups **Default** and **Certificate-Gateway.**
2. In the group inventory, select the check box against the group you want to delete.
3. Click the (**Delete**) icon in the command bar to delete the Group.
   A confirmation pop-up is displayed. Click the **Yes** button to proceed.

   The group is deleted and a confirmation message displays.

Configuring Certificates

• Configuring Certificate Settings
• Configuring Certificate Attributes
• Configuring Certificate Profiles
• Managing Certificate History
• Managing Expired Certificates

Configuring Certificate Settings

Configuring Password Vault

The password vault option is used to store all certificate passwords of the selected ADC devices. All the password-protected certificates that are discovered, will be decrypted and pushed to the discovery grid in the AppViewX Inventory. This happens only if passwords are matched with passwords that are stored in the vault.

Before you Begin

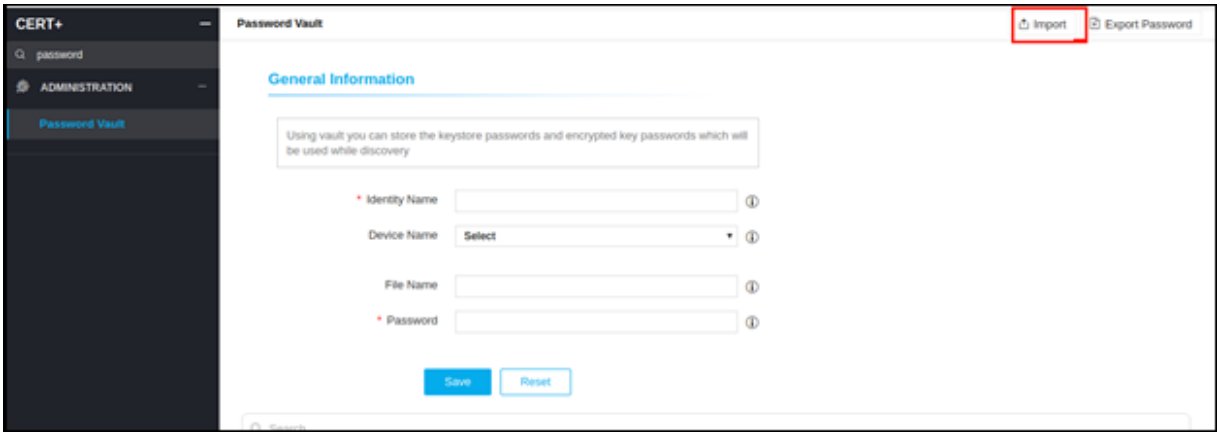
The prerequisites for configuring the Password Vault in AppViewX as are follows:

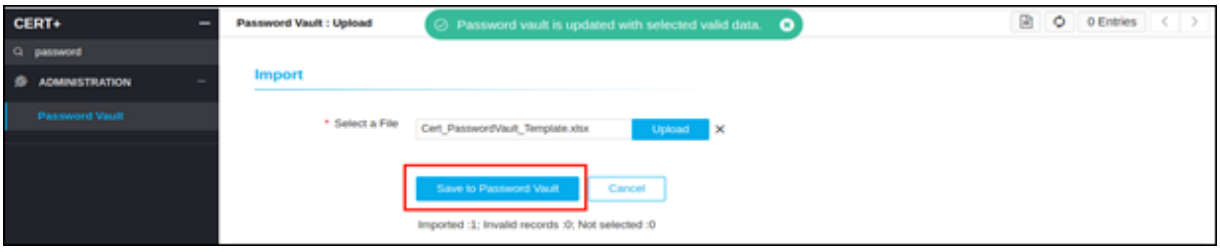
• A valid certificate password for password-protected certificates to decrypt.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** and click **Password Vault**.
2. On the screen that is displayed, enter an **Identity Name** of the password you want to add in the vault.
3. From the **Device Name** dropdown list, select the ADC device whose password-protected certificate details you want to store.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **File Name** field, enter a certificate file name to help users identify it.
5. In the **Password** field, enter the password that is associated with the certificate.
6. Click **Save**.
7. To import a file (in XLS or CSV format) with a list of all certificate passwords, on the top-right corner, click **Import**. This option is used to store the certificate passwords directly in the vault instead of adding them manually.





8. Click **Export Password** on the top-right to export all stored certificate passwords from the vault as a zip file to your computer.
9. To modify the existing details, Click **Edit.**
10. To update the password, click **Update.**
11. To delete the password details, click **Delete.**

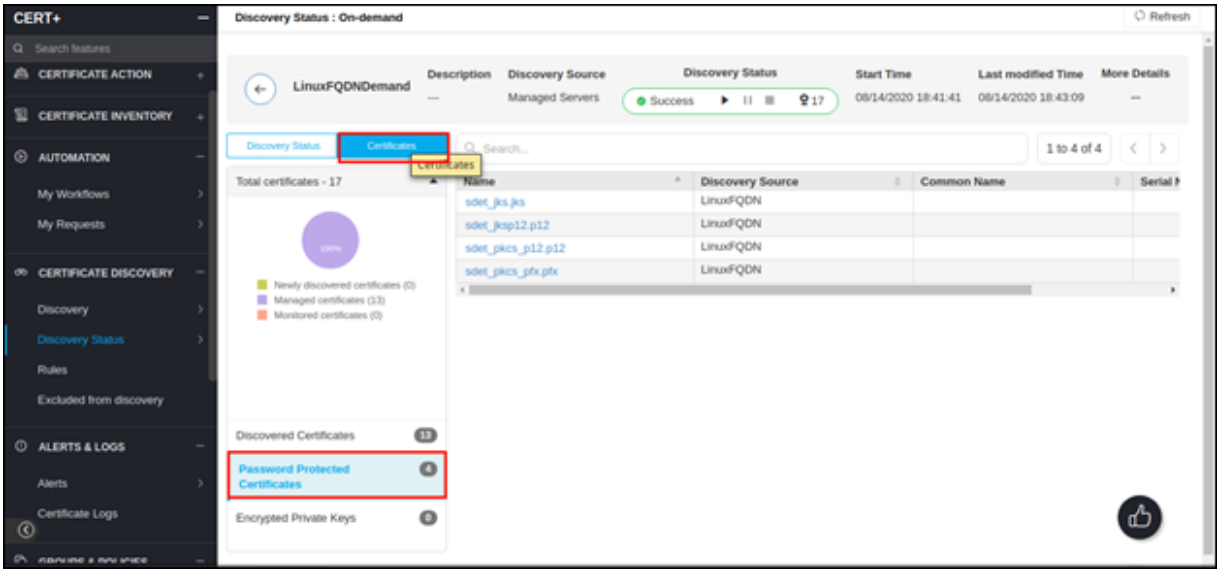
Password Protected Certificates

Password mismatch or password unavailable in the vault for the password-protected certificates that are discovered will be under the password-protected certificates section.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery Status** > **OnDemand**.
2. Click on the **discovery name** under discovery inventory.
3. Click **Certificates** under the tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. To view all password-protected certificates, click **Password Protected Certificates.**



Configuring Certificate Attributes

Certificate Attributes are a way of creating additional placeholder fields which can be used to track a certificate. An administrator can create one or more fields that a requester enrolling a certificate can fill and use for future tracking.

Prerequisites for Creating and Configuring Certificate Attributes

The prerequisites for configuration the certificate attributes are as follows:

- Certificate attributes are CA or organization-specific attributes, apart from the CSR parameters.

  Once configured, these attributes will be shown to collect values during certificate enrollment.

  Business unit-specific parameters can be stored for quick filtering and auditing.

Understanding the Certificate Attributes Inventory

To view the certificate attributes inventory, go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Attributes**.
The **Certificate Attributes** page is displayed.

For the certificate attributes added, the inventory displays the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Uunderstanding the Certificate Attributes Inventory

Fields	Description
Label Name	Attribute name that will be displayed in the certificate enrollment form
Key ID	Unique identifier key assigned to the attribute
Mandatory	Indicates if the attribute is a mandatory field
Expiry Configuration Associated	
Actions	Given below is a description of what each icon in the **Actions** field stands for: • : This indicates the certificate attribute will not be displayed on the certificate enrollment page. This is only an indicative icon and not clickable. • : This indicates the certificate attribute will be displayed on the certificate enrollment page. This is only an indicative icon and not clickable. • : To edit the details of a certificate attribute, click this icon. • : To delete a certificate attribute, click this icon.

Creating Certificate Attributes

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Attributes**.
   The **Certificate Attributes** page is displayed.
2. From the **Certificate Attributes** section, click **Add New**.
   The **Certificate Attributes** dialog box is displayed.
3. For the attribute to be added, enter/select the corresponding details.

Field descriptions for Certificate Attributes

Fields	Description
***Label Name**	Attribute name which will be shown during certificate enrollment. E.g. Email Contact, Owner.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Label name should not start with special characters. No special characters except -, _ and spaces are allowed.
***Key ID**	Unique key for the attribute. Key ID must not start with special characters. No special characters except -, _ are allowed. **Important:** Once specified, the **Key ID** cannot be updated.
Field Type	From the dropdown list, from the following options, select the input field type: • **Text** • **Dropdown** • **Date**
Mandatory	Enable if this field needs to be mandatory.
Default Value	This field is displayed when **Field Type** = **Text**. Enter the default text that will be pre-populated in the text field.
***Default Value(s)**	This field is displayed when **Field Type** = **Dropdown**. Enter a comma-separated list of values that will be displayed in the dropdown list.
Default Date	This field is displayed when **Field Type** = **Date**. Use the calendar widget ( ) to select the default date and time values that will be displayed for the field.
Show in Enrollment Form	To show this attribute in the **Certificate Attributes** section of the certificate enrollment form, turn on this toggle button.

4. Click **Save**.
   The attribute is listed in the **Certificate Attributes** inventory (explained here). The attributes can b displayed on the certificate enrollment page as well as in the certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Modifying Certificate Attributes

To edit the details of a certificate attribute:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Attributes**.
   The **Certificate Attributes** page is displayed.
2. From the certificate attributes inventory, for the required attribute, from the **Actions** column, click .
   The **Certificate Attributes** dialog box is displayed with the existing certificate attribute details.
3. Modify the details, as required, and click **Update**.

> **Important:** The **Key ID** field is disabled for editing.

Deleting Certificate Attributes

To delete a certificate attribute:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Attributes**.
   The **Certificate Attributes** page is displayed.
2. From the certificate attributes inventory, for the required attribute, from the **Actions** column, click .
   The **Certificate Attributes** dialog box is displayed with the message **Do you want to delete the certificate attribute?**
3. Click **Delete**.

Configuring Certificate Profiles

AppViewX Cert+ offers administrators capability to define the type or purpose of a certificate through Certificate Profiles. An administrator can configure multiple Profiles defining the Key Usage and Extended Key Usage for a certificate enrolled through AppViewX. The Profiles defined are applicable on Certificates enrolled through AppViewX CA or Custom CA.

An Administrator can white label AppViewX CA through Custom CA.

Prerequisites

Following are the points needed to be known before starting to configure Certificate profile -

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Certificate profiles configure Key usage extensions that define the purpose of the public key contained in a certificate.
- Once configured, these profiles would be used to define Key Usage and Enhanced Key Usage while the signing a CSR through AppViewX CA and white labeled AppViewX CA or Custom CA.
- System comes prebuilt with three profiles corresponding to a standard Server Authentication, Client Authentication and CodeSigning Certificate.

Configuring Certificate Profiles

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Profile**.
2. Click **+ Add** icon on the top right corner.
3. Configure the **General Information** details as follows:

General Information - Field Description Table

Field	Description
***Name**	Unique name to identify the profile. Profile name should not start with special characters. Can contain only alphanumeric characters, no special characters except -, _, . are allowed.
***Purpose/Usage**	Certificate Type to which the Key Usage extensions are signed with. For example: Server or Client.
**: Mandatory fields*	

4. Configure the **Key Usages** as given below.

Key Usages - Field Description Table

Field	Description
***Critical**	Enable this field to sign the Key Usage extensions as **critical**.
***Key Usage(s)**	Key Usage extensions along with which the CSR is signed.
**: Mandatory fields*	

5. Configure the **Extended Key Usages** as given below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Extended Key Usages - Field Description Table

Field	Description
***Critical**	Enable this field to sign the Extended Key Usage extensions as **critical**.
***Extended Key Usage(s)**	Extended Key Usage extensions along with which the CSR is signed.
Enable Custom	To enable custom OID for the certificate profile, select this checkbox. Here, a custom Object Identifier (OID) is used to define custom policies for the certificate profile that certificates must adhere to.
***Custom EKU Values**	This field is displayed only when the **Enable Custom** checkbox is enabled. Enter the custom OID(s) that will be applied to this certificate profile. To specify more than one OID for the profile, enter a comma-separated list of the custom OIDs.
**: Mandatory fields*	

6. To enable additional **Custom Extensions** for this certificate profile, turn on the **Enable Custom Extensions** toggle.
   Custom Extensions in digital certificates refer to additional, non-standard attributes added to a certificate to support specific organizational or application requirements. These extensions extend the functionality of certificates beyond the standard fields and extensions defined in X.509 specifications.
7. In the **Policy ID** section, enter the policy id in the field..
8. Click **Save**.
   At the time of certificate enrollment, if you choose a certificate profile with custom OID and/or extensions:
   a. Choose this profile at the time of certificate enrollment.
   b. Complete certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. In the holistic view, click

to view the certificate details.

In the certificate details, the **CRL distribution points** field will give you the custom OID details and the **Authority Information Access** field will give you the custom extension details, as applicable.

Updating a Certificate Profile

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Profile**.
2. Under Administration, select **Certificate Profile**.
3. Click on the profile that needs to be edited.
4. Edit existing values.
5. Click **Update.**

Deleting a Certificate Profile

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Certificate Profile**.
2. Click (**Delete**) against the Profile to be deleted.
3. Click **Yes** in the **Delete Confirmation** pop-up.

Managing Certificate History

AppViewX lets you manage certificate status values after certificate renewal, reissuance, regeneration, or revocation. Certificate history is a record of a certificate's lifecycle, including details of its issuance, renewal, reissuance, regeneration, and revocation. Maintaining certificate history helps organizations track changes, audit compliance, and manage security effectively. The corresponding user interface settings in AppViewX help determine whether historical records are maintained and how certificates transition between different statuses.

Viewing Certificate History

1. Go to (**Menu**) > **CERT+** > **Certificate Inventory** > certificate type (for example, **Server**). Certificate inventory for the selected certificate type is displayed.
2. To open the holistic view of a certificate (where certificate history can be viewed), click the **Common Name** of the required certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. In the certificate holistic view, from the toolbar, click **History**.
   The **Certificate History** dialog box is displayed.

Managing Certificate History

> **Important:** If auto-archival settings have been enabled for renewed/regenerated certificates, the original certificates are moved to the Archived Inventory, rather than being deleted. Currently, reissued certificates are excluded from the scope of auto-archival settings.

To retain the history of a certificate:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **History of Certificates**.
2. In the **Manage Certificate History** section, for **Do you want to maintain the history of certificate after its renew/reissue/regeneration?**, select **Yes**.
3. From the end of the page, click **Save**.

Managing Certificate Status

> **Important:** If auto-archival settings have been enabled for renewed/regenerated/revoked certificates, the original certificates are moved to the Archived Inventory. Currently, reissued certificates are excluded from the scope of auto-archival settings.

For Renewed/Reissued/Regenerated Certificates

AppViewX lets you move renewed/reissued/regenerated certificates from the **Managed** state to the **Monitored** state after a fixed number of days after renewal/reissue/regeneration. This helps free up license space, thus resulting in optimal license usage.

To manage the certificate status for renewed/reissued/regenerated certificates:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **History of Certificates**.
2. In the **Manage Renewed/Reissued/Regenerated Certificate Status** section:

   a. For **Do you want to move Renewed/Reissued/Regenerated certificates from Managed to Monitor?**, select **Yes**.

   b. In the **Number of days after Renewal/Reissuance/Regeneration** (mandatory) field, enter how many days after renewal/reissue/regeneration should a certificate's status change from **Managed** to **Monitored**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Valid values for this field: **0** - **1999**

> **Note:** The certificate status transition is timestamp-driven and triggered by a scheduler cron job. For certificates renewed, reissued, or regenerated, the status transition will occur based on the configured **Number of days after Renewal/Reissuance/Regeneration**.
> - If the configuration is set to **0 days**, the transition happens immediately after the cron job executes.
> - For existing certificates (renewed, reissued, or regenerated prior to this configuration), the status transition will not be immediate even if **Number of days after Renewal/ Reissuance/Regeneration** = **0**. Their status will transition only after the cron job executes at its scheduled time.

3. From the end of the page, click **Save**.

For Revoked Certificates

To manage the certificate status for revoked certificates:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **History of Certificates**.
2. In the **Manage Revoked Certificate Status** section:

   a. For **Do you want to move Revoked certificates from Managed to Monitor?**, select **Yes**.

   b. In the **Number of days after revocation** field, enter how many days after revocation should a certificate's status change from **Managed** to **Monitored**.
   Valid values for this field: **0** - **1999**

> **Note:** The certificate status transition is timestamp-driven and triggered by a scheduler cron job. For certificates renewed, reissued, or regenerated, the status transition will occur based on the configured **Number of days after revocation**.
> - If the configuration is set to **0 days**, the transition happens immediately after the cron job executes.
> - For existing certificates (renewed, reissued, or regenerated prior to this configuration), the status transition will not be immediate even if **Number of days after revocation** = **0**. Their status will transition only after the cron job executes at its scheduled time.

3. From the end of the page, click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Managing Expired Certificates

Deleting Expired Certificates

Important: If auto archival settings have been enabled for expired certificates, the expired certificates are not deleted; instead, they are moved to the Archived Inventory.

To set up automatic deletion of expired certificates:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Expired Certificates**.
2. In the **Expired certificate** section, for **Do you want to delete the expired certificates?**, select **Yes**.
3. From the end of the page, click **Save**.

Managing Expired Certificate Status

Important: If auto archival settings have been enabled for expired certificates, expired certificates are moved to the Archived Inventory; there is no change in the certificate status.

To set up automatic certificate status management for expired certificates:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Expired Certificates**.
2. In the **Manage Expired Certificate Status** section:
   a. For **Do you want to move Expired certificates from Managed to Monitor?** option, select **Yes**.
   b. In the **Number of days after expiry** (mandatory) field, enter how many days after expiry should a certificate's status change from **Managed** to **Monitored**.
   Valid values for this field: **0** - **1999**

Note: Certificate status will change only after the scheduled job has successfully run, based on the **Number of days after expiry** configured.

Deleting Expired Root and Intermediate Certificates

Note: Currently, root and intermediate certificates are excluded from auto-archival settings, which apply only to end-entity certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To automatically delete expired root and intermediate certificates:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Expired Certificates**.
2. In the **Expired root and intermediate certificate** section, for **Do you want to delete the expired root and intermediate certificates?**, select **Yes**.
3. From the end of the page, click **Save**.

Configuring and Managing Devices

Note: For prerequisites to manage ADC, Servers, Firewall, Cloud devices into AppViewX Device inventory, click here.

Managing a device in the AppViewX device inventory allows administrators or users of the platform to discover certificates currently in use on the devices. Also, an administrator or user can provision or push a certificate to the device through the platform.

- Configuring ADC Devices
- Configuring and Managing Servers
- Configuring and Managing Firewalls
- Configuring Switches
- Configuring Routers
- Configuring and Managing Cloud Devices
- Configuring WAFs

Configuring ADC Devices

- Adding A10 Device
- Adding Akamai Device
- Adding Amazon ELB
- Adding Array Device
- Adding AVI Device
- Adding BigIQ Device
- Adding Cisco Device
- Adding Citrix Device
- Adding Cloudflare Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Adding F5 Device
- Adding F5XC Device
- Adding HAProxy Device
- Adding InfoBlox Device
- Adding NginxPlus Device

Adding A10 Device

To add an A10 device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **A10** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Type	Description	Validation
Module	Check box	SLB / GSLB Module.	NA
Device name	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Communication	Radio button	Devices can be accessed using an IP address or FQDN.	NA
IP Address	Text	The IPv4 address of the device.	The IP address should be in the right format.
FQDN	Text	The FQDN of the device.	the FQDN should be in a valid format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
Cert Sync	Radio button	Managed: The certificates of the device can be managed. Monitored: The certificates of the device can be monitored. Ignored: The certificate sync can be ignored.	NA
AppViewX Group Sync	Check box	This should be enabled if the user wants to sync the devices within the device group.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credential List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry:** The user should enter the username and password. **Credential List:** The user can select the credential details which are already stored in the credential inventory page.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
***Username**	Text	If manual entry is selected, the user name should be entered by the user.	NA
***Password**	Text	If manual entry is selected, the password should be entered by the user.	NA
Enable password	Text	Enable password of the A10 device.	NA
**: Mandatory fields*			

6. Enter the field information in the **Secondary device information** section.
7. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

Secondary device information Section - Field and Description Table

Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

8. Click **Save**.

Adding Akamai Device

To add an Akamai device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **Akamai** from the left sidebar.
4. Enter the required details for the device addition.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Device Addition - Field and Description Table

Name	Type	Description	Validation
***Device name**	Text	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
***Client token**	Text	Client token of the Akamai device.	NA
***Client secret**	Text	Client secret of the Akamai device.	NA
***Access token**	Text	Access token of the device.	NA
***URL**	Text	Valid URL of the Akamai device.	NA
**: Mandatory fields*			

5. Click **Save**.

Adding Amazon ELB

To add an Amazon ELB:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select Amazon ELB from the left sidebar.
4. Enter the field information in the **Basic information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Basic information Section - Field and Description Table

Name	Type	Description	Validation
***Account name**	Text	The account name of the AmazonELB device.	NA
***Account number**	Text	Account number of the AmazonEB device.	Numbers only.
Device description	Text	Description about the AmazonELB account.	NA
Cert Sync	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Mandatory	Description	Validation
***Credential type**	Dropdown	Yes	**Manual entry**: The user should enter the Access key ID and Secret access key. **Credential List**: The user can select the credential details which are already stored in the credential inventory page.	NA
***Access key id**	Text	Yes	Access key id of the AmazonELB device.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Mandatory	Description	Validation
***Secret access key**	Text	Yes	Secret access key of the AmazonELB device.	NA
**: Mandatory fields*				

6. Enter the field information in the **Key information** section.

Key information Section - Field and Description Table

Name	Type	Description	Validation
***Service region**	Dropdown	Service region of the AmazonELB device.	NA
**: Mandatory fields*			

7. Click **Save**.

Adding Array Device

To add an Array device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **Array** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Description
***Modules**	Select modules checkbox. The values are • SLB • GSLB
***Device name**	Unique name of the device to be added. **Note:** Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
Data center	Enter the Datacenter name where the device is configured. The default value is Absecon. **Note:** Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Communication	Select the communication method for accessing devices, either through an IP address or FQDN.
***IP Address**	Enter the IPv4 address of the device. **Note:** The IP address must be in the correct format.
***API Port**	Enter the communication port of the device. **Note:** Only the numbers are allowed.
Cert Sync	Select the certificate sync option: • **Managed**: The certificates of the device can be managed. • **Monitored**: The certificates of the device can be monitored. • **Ignored**: The certificate sync can be ignored.
LB Sync	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.
**: Mandatory fields*	

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Description
***Credential type**	**Manual entry:** The user should enter the username and password.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
	Credential List: The user can select the credential details which are already stored in the credential inventory page.
***Username**	Enter the user name of the device.
***Password**	Enter the password of the device.
**: Mandatory fields*	

6. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Description
***Secondary / Failover / Sync group**	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.
**: Mandatory fields*	

7. Click **Save**.

Adding AVI Device

To add an AVI device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **AVI** from the left sidebar.
4. Enter the field information in the **General information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Module**	Check box	SLB / GSLB Module.	NA
***Device name**	Text	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Communication	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The IPv4 address of the device.	The IP address should be in the right format.
FQDN	Text	The FQDN of the device.	the FQDN should be in a valid format.
Cert Sync	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
LB Sync	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.		
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential inventory page.	NA
***Username**	Text	If manual entry is selected, the user name should be entered by the user.	NA
***Password**	Text	If manual entry is selected, the password should be entered by the user.	NA
Enable password	Text	Enable password of the AVI device.	NA
**: Mandatory fields*			

6. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		Manual entry: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	

7. Click **Save**.

Adding BigIQ Device

To add a BigIQ device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **BigIQ** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Device name**	Text	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
***IP Address**	Text	IP Address of the BigIQ device.	IP address should be in IPv4 format.
Data center	Text	Datacenter name where the device is configured. Default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential inventory page.	NA
***Username**	Text	Username of the BigIQ device.	NA
***Password**	Text	Password of the BigIQ device.	NA
**: Mandatory fields*			

6. Click **Save**.

Adding Cisco Device

To add a Cisco device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **Cisco** from the left sidebar.
4. Enter the field information in the **General information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Module**	Check box	SLB Module.	NA
***Device name**	Text	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
***IP Address**	Text	IP Address of the BigIQ device.	IP address should be in IPv4 format.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Cert Sync**	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		Credential List: The user can select the credential details which are already stored in the credential inventory page.	
***Username**	Text	Username of the Cisco device.	NA
***Password**	Text	The password of the Cisco device.	NA
**: Mandatory fields*			

6. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory. **Manual entry**: The user can use this option to add the peer devices manually.	NA

7. Click **Save**.

Adding Citrix Device

To add a Citrix device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **Citrix** from the left sidebar.
4. Enter the field information in the **General information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Module**	Check box	SLB / GSLB Module.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The IPv4 address of the device.	The IP address should be in the right format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
***Cert Sync**	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential inventory page.	NA
***Username**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
**: Mandatory fields*			

6. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

7. Click **Save**.

Adding Cloudflare Device

Before You Begin

Prerequisites

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites for Managing Cloudflare devices on AppViewX are:

- **Version Supported**: v4
- **IP Address/FQDN**: NA
- **User Privilege**: Api Token

Note:

When creating a Cloudflare API token for managing load balancing, the following minimum permissions should be granted:Permissions:

1. **Zone-level Permissions**: Load Balancing: Read/Edit
   This permission allows the token to manage and modify load balancer configurations within specified zones.
2. **Account-level Permissions**: Load Balancing Pools and Monitors: Read/Edit
   This permission enables the token to manage and modify load balancing pools and health monitors within specified accounts.

Resources:

Account Resource: Include the specific account(s) that should be accessible using this token.

Zone Resource: Include all zones where load balancing management is required.

- **Enable Password**: NA
- **License Check**: No
- **Services and Ports for AppViewX Communication**: Port 443, Outbound Internet access is required to manage the cloudflare
- **Internet Access/Proxy if Required**: Required
- **Location from which Certificates are discovered if managed**: NA

Web Browser Requirement

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	118.0.1 (64-bit) or later
Google Chrome	117.0.5938.134 (Official Build) (64-bit) or later

ACF Permission

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Ensure the following ACF permission is available to add and manage devices:

- ADC > Inventory > Add / Modify
- ADC > Device group > Add / Modify

You can check this under any of the following menus:

- **Old menu**: menu > Accounts > Role
- **New menu**: menu > Platform > IDENTITY > Role

To associate ACF permissions with a role, see Platform User Guide.

Adding Cloudflare Device

To add a Cloudflare device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **Cloudflare** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Description
***Device name**	Unique name of the device to be added. **Note:** Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Access Url	Access URL of Cloudflare.
***Account Id**	Account ID of Cloudflare.
Data center	Datacenter name where the device is configured. The default value is Absecon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
	Note: Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
LB Sync	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.
**: Mandatory fields*	

5. Enter the field information in the **Credentials** section.

Credentials Section - Field and Description Table

Name	Description
***Credential type**	**Manual entry**: The user should enter the API token.
***Api Token**	API token. Required token permissions are: • Zone Level: Load Balancing • Account Level: Load Balancing Pool and Monitors
**: Mandatory fields*	

6. Click **Save**.

Validating the Cloudflare Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
2. Search the device name and validate whether the device is added successfully.

What's Next

• Check the Logs for transaction ID and details

Adding F5 Device

To add an F5 device:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, click the **F5** icon.
4. Enter the field information in the **General information** section.

   a. For the device type **Device/Tenant**:

General information Section for "Device/Tenant" Device Type - Field and Description Table

Name	Type	Description	Validation
Device Type	Drop-down	When you select Device Type as Device/ Tenant, you will need to provide the relevant device information in the following fields.	NA
***Module**	Check box	LTM / BIG-IP DNS Module.	NA
VCMP Guest	Check box	To add a device as a vcmp guest, this checkbox should be checked.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The ipv4 address of the device.	The IP address should be a valid IPv4 format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
***Cert Sync**	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	NA
DNSSEC sync	Radio button	By default, the Ignored option is selected. If your ADC acts as an authoritative DNS server, then select the Managed option to manage the DNSSEC Zones and Keys (KSK and ZSK).	
AppViewX Group Sync	Check box	This should be enabled if the user wants to sync the devices within the device group.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

b. For the device type **Host**:

General information Section for "Host" Device Type - Field and Description Table

Name	Type	Description	Validation
Device Type	Drop-down	When you select Device Type as Host, you will need to provide the relevant device information in the following fields.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
Host Type	Radio button	Select any of the following host types: • vCMP Host - Enables the running of multiple virtual instances of BIG-IP software on a single physical device • rSeried Host - A host type representing the F5 rSeries hardware platform, designed for high-performance application delivery and security. • Velos Partition - A logical partition on the F5 VELOS platform, allowing for the segmentation of resources and management of multiple tenants within a single VELOS chassis.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The ipv4 address of the device.	The IP address should be a valid IPv4 format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
**: Mandatory fields*			

c. For the device type **Controller**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General information Section for "Controller" Device Type - Field and Description Table

Name	Type	Description	Validation
Device Type	Drop-down	When you select Device Type as Controller, you will need to provide the relevant device information in the following fields.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The ipv4 address of the device.	The IP address should be a valid IPv4 format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		inventory page. For more details on secure authentication, refer to Platform User Guide.	
***Username**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
Token based authentication	Toggle button	To access the device REST API using token.	NA
**: Mandatory fields*			

6. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

7. Click **Save**.

Adding F5XC Device

Before You Begin

Prerequisites

- **Version Supported**: NA
- **IP Address/FQDN**: FQDN
- **User Privilege**: admin
- **Enable Password**: NA
- **License Check**: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Services and Ports for AppViewX Communication**: NA
- **Internet Access/Proxy if Required**: Internet access required
- **Location from which Certificates are discovered if managed**: NA

Web Browser Requirement

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	118.0.1 (64-bit) or later
Google Chrome	117.0.5938.134 (Official Build) (64-bit) or later

ACF Permission

Ensure the following ACF permission is available to add and manage devices:

- ADC > Inventory > Add / Modify
- ADC > Device group > Add / Modify

You can check this under any of the following menus:

- **Old menu**: menu > Accounts > Role
- **New menu**: menu > Platform > IDENTITY > Role

To associate ACF permissions with a role, see Platform User Guide.

Adding F5XC Device

To add an F5XC device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is selected.
2. Click the **(Add)** icon.
3. From the **Device details** page, select **F5XC** from the Vendors list.
4. Enter the field information in the **General information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General information Section - Field and Description Table

Name	Description
***Device name**	Enter a unique name of the device to be added. Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
***Device URL**	Enter URL to access the device.
Data center	Select a data center name where the device is configured from the list or enter a new datacenter name. The default value is Absecon. Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Cert sync	Choose from any of the following: • **Managed -** AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • **Monitored -** AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • **Ignored -** AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
LB Sync	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.
**: Mandatory fields*	

5. In the **Services** section, select from **Distributed App** or **DNS Management** service type.

Note:
- More than one service type can be selected but **Cert Sync** feature is applicable only for **Distributed App** service type.
- Only on selecting **Distributed App** service, certificates are discovered and profiles created.

6. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

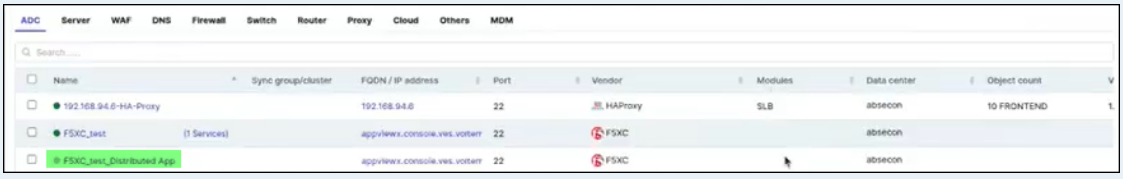
Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential Type**	Dropdown	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential inventory page. For more details on secure authentication, refer to Platform User Guide.	NA
***User Name**	Text	The user name of the device.	NA
***Token Auth**	Text	Authentication token to access the device REST API using token.	NA
**: Mandatory fields*			

7. In the **Vendor Specific Details,** enter namespace(s) to scope for CLM operation. Namespaces must start with a letter, can contain lowercase letters, numbers, hyphens, and must end with a letter or number.

> **Note:** The **Namespace** field is optional. If specified, CLM operations (certificate discovery, profile creation, etc.) are limited to the listed namespaces. If not, certificates are discovered from all namespaces, profiles created, and CLM operations performed for all namespaces.

8. Click **Save**.

> **Note:** On adding an F5XC device (F5XC_test), it will appear as the primary device while the service (F5XC_test_Distributed_App) is also displayed as shown:
>
> 
>
>
> Click the **Refresh** button if you do not see the service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Discovering Certificates

- To discover certificates (on-demand/scheduled), enable **Distributed App** service.
- Certificates and connectors are discovered from either all namespaces or a specific provided namespace on the F5XC device. This includes certificates from the root, intermediate, and server inventories, as well as their associated connectors within those namespaces.

> **Note:** Discovered certificates cannot be re-pushed to other namespaces due to lack of private keys.

- Profiles are created considering the namespaces, HTTP, and TCP LB. Sample profiles:
  - deviceName:{tenant_id}:{name_space_name} - Default profile
  - deviceName:{tenant_id}:{name_space_name}:http_lb:{lbname}
  - deviceName:{tenant_id}:{name_space_name}:tcp_lb :{lbname}

> **Note:**
> - Discovery does not export private keys.
> - One LB can have multiple certificates.
> - The same certificate can be mapped to multiple HTTP and TCP LB.

- Default profile is created for a namespace to support push operation.
- Load balancer profile is created for a namespace to support bind operation.
- Config sync triggers a discovery and manages the profiles based on the cert sync status.
- Filters and rules can be applied for the discovery.

Pushing Certificates

Certificate naming convention

- The certificate name must be unique within the namespace. It cannot be changed during an update.
- If certificate with same name already exists for a given namespace, you will see, *Object already exists,* message.
- The **certificate name** field must start with an alphabet, contain lower case alphanumeric characters or "-", and end with an alphanumeric character.

Certificate Push Format

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Certificates must be pushed in the **PEM format**, including the PEM headers.
- You can push a certificate along with its private key.

Private Key Handling

- The request must include the private key. If not provided, the request will be rejected.
- Supports `private_key: clear_secret_info`

Limitations

- The API does not support blindfolding private keys (i.e., encrypting them with `blindfold_secret_info_internal`).

Trust Chain Push Options

- You can optionally include root and intermediate certificates during a server certificate push.

  Root and intermediate certificates can be pushed separately by enabling the support from the respective inventory.
- By default, only the server certificate is pushed (root and intermediate are unchecked by default).
- When enabled, users can choose:
  - To push the certificate as a bundle (server, intermediate, and root certificates).
  - To use the trust chain already available in the F5XC inventory for the selected profile namespace.

Intermediate Certificate Chain Push Behavior

- The **Push as Intermediate Certificate Chain** option is available only if:
  - The selected profiles belong to the same namespace, device, and tenant.
  - If profiles from multiple namespaces/devices/tenants are selected, this option will be disabled.
- If a user selects this option and later adds a new profile that is incompatible (e.g., from a different namespace), the connector cannot be saved.
- When selected:
  - The user can choose an existing trust chain from a dropdown.
  - If no trust chain data is available, the option cannot be selected.

Certificate Overwrite and Replacement

- If a certificate with the same name already exists in the namespace, the operation will fail—regardless of whether the content is identical or not.
- In such cases, check if **`overwrite`** is enabled in the request:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Direct removal of a certificate association from a load balancer is **not supported**—only replacement and re-binding are allowed.

Note: The system supports flexible certificate deployment strategies aligned with trust chain management in F5XC.

Binding Certificates

- Load Balancers (LBs) do not store certificates directly. Instead, they reference certificate objects by name.
  - If a certificate with the same name is already associated with one or more LBs, updating or rotating the certificate will automatically apply the changes to all referencing LBs—no additional binding is required.
- When updating a certificate object, the LBs referencing it will immediately start using the updated version, since the reference by name remains unchanged.
  - For a selected LB profile, if the certificate name is already bound, re-binding is not necessary.
- The system only supports overwriting and binding a new certificate to the LB.
  - Unbinding or removing a certificate from an LB is **not supported** as part of the push-and-bind operation.
- Multiple certificates can be attached to the same load balancer.
- A single certificate can also be used by multiple load balancers (within the same namespace).
- When F5XC certificate bind fails, it will display, *Certificate is invalid*, message.

Backing Up Certificates

As the private key cannot be exported—and is mandatory for certificate push—backing up the certificate is not applicable.

Backup is performed only in specific use cases, especially when a new certificate is pushed. In such cases, the backup operation checks whether the certificate is newly pushed or if it already existed before setting the rollback eligibility to **true**. This **partial backup** occurs **only** when the certificate is new and is **not already associated** with the load balancer.

Rolling Back Certificates

When certificates are pushed to the system, a rollback mechanism can be used if the pushed certificates are not successfully bound to a load balancer. This ensures that only fully applied and active certificate changes are retained.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Validating F5XC Device Addition

After adding the device, you can validate the device by searching the device in the device inventory.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
2. From the device inventory page, search for the added F5XC device name.

Adding HAProxy Device

Prerequisites

1. Ensure that the following packages are installed on the HAProxy machine:
   - socat
   - systemctl
   - ps
   - sftp
   - setfacl (optional)
2. As **SFTP** is used for file transfers (certificate push), it is crucial to ensure that SFTP is properly configured for the logged-in user.
   a. From the cloud connector, use the `sftp` command to test the connection to an SFTP server. Open your terminal and type:

      ```
      sftp username@hostname
      ```

   b. Use the `put` command to upload the file to the remote server: put localfile /path/to/remote/directory
3. Do not limit SFTP sessions to a single connection. Allowing only one SFTP session at a time can lead to failures during push operations. To prevent this, it is advisable to modify the settings in `/etc/security/limits.conf` to permit up to 5 simultaneous connections.

   Add `sftptest hard nproc 5` to the limits.conf. Log out and log back in to validate the SFTP connections. If this does not work, restart the SSH service and retry the use case.

   If the above step does not work, add or modify the *MaxSessions* to 5 in the sshd_config or any included file in the sshd_config.
4. Ensure that the target IP/FQDN is accessible from the cloud connector (SaaS) or from vendor pods (on-prem) and the port is open.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Certificates located in paths without the necessary user permissions cannot be detected. Therefore, either update the configuration files to reference certificates in accessible paths or modify the file permissions to ensure the certificates are accessible.
6. The user must have appropriate access to the configuration file and certificates. If direct access is not permitted, elevated privileges must be granted for the commands listed in the Commands requiring Access Elevation section.

Adding HAProxy Device

To add an HAProxy device:

1. Go to (**Menu**) > **CERT+** > **Device Management**.
   By default, the ADC tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **HAProxy** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Modules**	Checkbox	Select a module.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication	Radio button	The communication mode that ADC devices can be added to AppViewX.	NA
***SSH Port**	Text	Communication port of the device.	Numbers only.
***IP Address**	Text	The IPv4/IPv6 address of the device.	IP address must be a valid IPv4/IPv6 address.
***FQDN**	Text	FQDN/hostname of the device.	FQDN value must be a valid FQDN/hostname.
Data center	Dropdown	Datacenter name where the device is configured. The default value is *absecon*.	Data center name can only contain alphanumeric

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
			characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Cert Sync**	Radio button	• **Managed:** The certificates of the device can be managed. • **Monitored:** The certificates of the device can be monitored. • **Ignored:** The certificate sync can be ignored.	NA
LB Sync	Toggle button	The LB Sync toggle button is enabled and modifiable only with an ADC+ license. In environments with a CERT+ only license, the toggle is disabled.	NA
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential Type**	Dropdown	• **Manual entry**: The user should enter the username and password. • **Credential List - AppViewX**: The user can select the credential details which are already stored in the credential inventory page.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		Note: • All other vault settings (BeyondTrust, Cyberark, Hashicorp Vault, Thycotic, and so on.) configured in the Credentials will be displayed in the dropdown. • If **Credential list - AppViewX** is selected, the *Credentials list dropdown field is displayed. Select any of the preconfigured credential values. • If **Credential list - HashiCorp** is selected, the *Credentials list dropdown field is displayed with credential type by default	
***User Name**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
**: Mandatory fields*			

6. Enter the fields in **Vendor Specific Details.**

Vendor Specific Details Section - Field and Description Table

Name	Type	Description	Validation
***Access Elevation**	Dropdown	• **None**: By default, None is selected. • **sudo**: sudo enablement is supported for CLM actions. LB operations do not currently support this functionality.	NA
***File Upload Temp Path**	Text	This field is displayed when **Access Elevation = sudo**. The path specified here will be used for push, bind, and CSR generation.	It must either be left empty or set to a valid Linux folder with an absolute path. The path should

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
			begin with a forward slash (/), and all folder separators must also use forward slashes.
*: Mandatory fields			

7. Click **Save**.

CSR Generation

When pushing a certificate where the private key is generated on the end device, ensure that the **Private key at end device** checkbox is selected, and specify the same location for the private key in the push screen.

Note: The key generated at the endpoint during CSR generation will permit read-only access for the owner of the file; no other user in the same user group or anyone else will have any permission.

Backing Up Certificates

- Copy the content of the configuration file and parse it to find the certificate locations.
- Download the certificates from the locations bind to SSL configurations under the frontend.
- Parse the certificates and store them under the backup properties.

Pushing Certificates

- After the push, a single file will be pushed to the endpoint, which has the content of the certificate chain (root, intermediate and server certs) appended with the private key.
- The following order of content is followed as a standard:
  - Server certificate
  - Intermediate certificate(s)
  - Root certificate
  - Private key

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

There is a provision to re-order the content. As the PEM file content requires the private key to appear at the beginning, a database script must be run to meet this requirement:

```
db.cert_metadata.update({_id:"CERT_VENDOR_BASED_CONDITIONS"},{"$set":
        {"map.adc_haproxy_push_private_private_key_at_first" : "true"}})
```

- A file is created at the haproxy endpoint in the user-configured location and the content will be written in that PEM file.
- When you choose the private key on the device, provide the absolute path of the server-generated private key on the UI screen.

Binding Certificates

Copy the config file content (haproxy.cfg) and update the certificate location using regex for the profile that is associated with an SSL bind directive under the front end. Upload the updated config file to the original location.

Note: If certificate and config file exist, file permissions are retained.

Restarting/Reloading Service

Once the new certificate is successfully bound in the configuration file, it will be used after the configuration is restarted or reloaded.

- **Restart**: Kills the process by closing all the connections immediately and starting a new process.
- **Reload**: It will not accept any new connections (stops listening on all the respective ports) and gracefully reloads the haproxy service.

Rolling Back Certificates

The rollback process follows the same push and bind flow, with certificate details retrieved from the backup properties created during the backup.

Commands requiring Access Elevation

```
find
mkdir
touch
stat
openssl
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
cat

rm

chmod

chown

ps

systemctl

cp

setacl (Optional)
```

Adding InfoBlox Device

To add an InfoBlox device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **Infoblox** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The IPv4 address of the device.	The IP address should be in the right format.
***FQDN**	Text	The FQDN of the device.	The FQDN should be in a valid format.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
LB Sync	Checkbox	Enable this toggle button to discover and manage the load balancer configurations.	
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential inventory page.	NA
***Username**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
**: Mandatory fields*			

6. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Type	Description	Validation
Secondary / Failover / Sync group	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

7. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Adding NginxPlus Device

To add an NginxPlus device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab is displayed.
2. Click the **(Add)** icon.
3. In the **Device details** page, select **NginxPlus** from the left sidebar.
4. Enter the field information in the **General information** section.

General information Section - Field and Description Table

Name	Type	Description	Validation
***Modules**	Check box	SLB	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication	Radio button	Devices can be accessed using an IP address or FQDN.	No
***IP Address**	Text	The IPv4 address of the device.	The IP address should be in the right format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Cert Sync	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

5. Enter the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry:** The user should enter the username and password. **Credential List:** The user can select the credential details which are already stored in the credential inventory page.	NA
***Username**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
**: Mandatory fields*			

6. Enter the field information in the **Authenticaion details** section.

Authenticaion details Section - - Field and Description Table

Name	Type	Description	Validation
Sudo Auth	Checkbox	Select the **Sudo Auth** checkbox in the to enable the Sudo authentication for a non-root user credentials.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
API Auth	Dropdown	This option allows the basic or token based authentication for API enabled devices. The options are: • **Basic Auth** - select this option to configure HTTP authentication with password. You can choose device credentials or manual entry. • **Token Auth** - select this option to enter the JSON Web tokens for token based authentication.	

7. Enter the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

Name	Type	Mandatory	Description	Validation
Secondary / Failover / Sync group	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

8. Click **Save**.

Configuring and Managing Servers

Configuring servers in the AppViewX Certificate Management module is essential for enabling secure, automated management of certificates across systems. Proper configuration ensures that servers can seamlessly integrate into the certificate lifecycle, reducing manual intervention and improving operational efficiency.

To provide guidance on how to set up servers for handling certificate operations to securely manage certificates and perform tasks efficiently, this section covers instructions for:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Adding a Server
- Deleting a Server
- Importing a Server
- Exporting a Server
- Managing a Server
- Unmanaging a Server
- Executing Fetch Config for Server
- Adding Device Credentials
- Configuring Device Setting

Adding a Server

This section describes the process of onboarding IIS and non-IIS web servers into AppViewX.

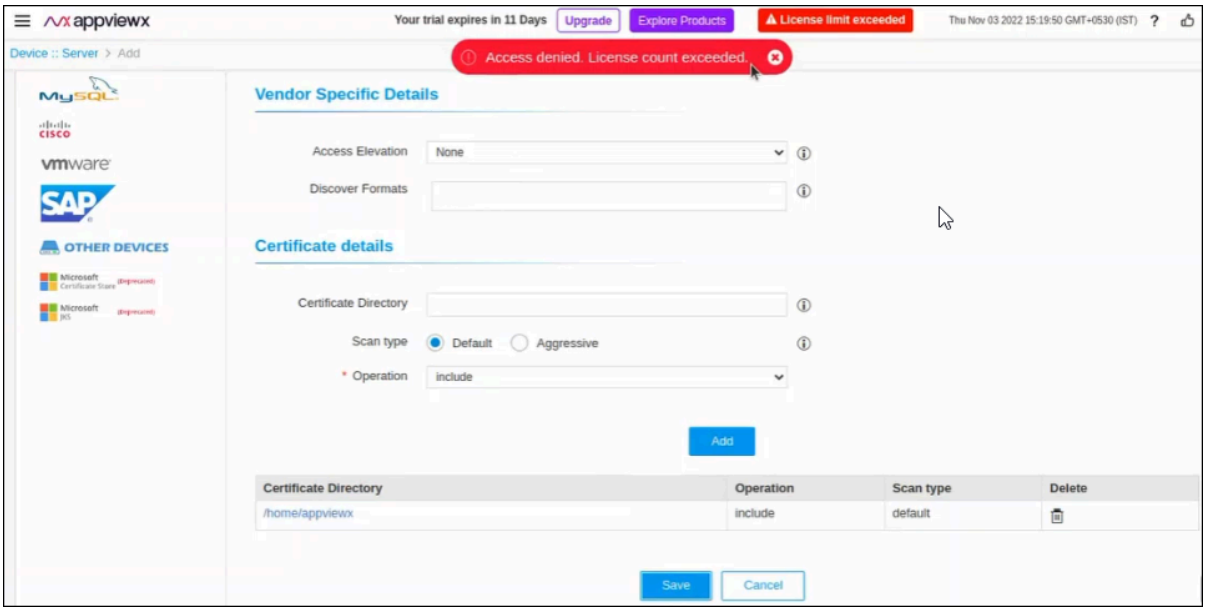
- Akamai
- Apache (Linux)
- Apache (Windows)
- Arbor
- CISCO
- Dell
- HP-ILO
- IBM
- JBoss
- Generic Linux
- Microsoft IIS
- Microsoft PC
- Microsoft Server
- Microsoft SQL
- MySQL
- NGINX
- Oracle
- Other Devices
- RabbitMQ
- SAP

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Tomcat (Linux)
- Tomcat (Windows)
- VMware
- Gigamon
- PingFederate

License Enforcement

AppViewX has enabled a feature to set a limit for the licensed certificates. If the number of certs exceeds this limit then the additional certs added to the inventory will be moved into the **Monitored** status.



- A red indicator labeled "**License Limit Exceed**" is displayed on the title bar of the page, if the limit has exceeded.
- A pop-up message "**Access denied. License count exceeded.**" is displayed on the click of the **Save** button while adding a new server device.
- All the new on-boarded server certs (Server/ADC/Firewall/WAF Device config sync) into the inventory will be mapped to the **Monitored** state.

Akamai

The Akamai CPS (Certificate Provisioning System) provides full life cycle management of SSL/TLS certificates for Akamai Secure Delivery Network applications.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

- Create authentication credentials. before using the API.
- To enable this API, choose the **Certificate Provisioning System** API service, and set the access level to **READ-WRITE**.
- Ensure your API credentials have the following grants: **CPS** and **Contracts-API_Contracts**.

Onboarding Akamai CPS Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Akamai** logo from the Vendors list.
   The **Akamai** server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the server name, a unique name for the device addition.
***IP address/ FQDN**	Enter the valid IP address or FQDN for device communication and integration with the Akamai CPS.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Akamai server.
Proxy	Select the checkbox to enable the secure proxy service.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. In the **Credentials** section, enter details as mentioned below.

Credentials - Field Description Table

Fields	Description
***Client token**	Enter the client token as provided by the vendor.
***Client secret**	Enter the client secret as provided by the vendor.
***Access token**	Enter the access token as provided by the vendor.
***API Version**	Enter the value, example cps/v2. (The same value is provided as the placeholder.)
*: Mandatory fields	

7. Click **Save**.
   The Akamai CPS device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Apache (Linux)

Prerequisites

1. Ensure that application/service users have the appropriate read/write permission to perform the CLM actions on the server device, if the access elevation is selected as **None**.
   When the access elevation is **sudo** or **dzdo**, all the commands used to perform the CLM operations will be executed with sudo or dzdo.
2. Verify that the commands needing sudo or dzdo access have been enabled on the server.
3. Ensure that the following packages are installed to facilitate device addition:
   - sudo/dzdo (optional, as per the access elevation selected)
   - timeout
   - base64
4. Ensure that the target IP address is accessible from the cloud connector and the port is open.
5. Make sure that the language setting for the Apache Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
6. Only certifiticates in .pem, .crt, and .cer formats and key files are discovered.
7. SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
8. Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.
9. Verify the existence of **httpd.conf** file in the system by scanning from root directory. Use the command: find / -name “httpd.conf”.
10. Check for the ServerRoot location in the **httpd** file. Make sure it holds forward slashes(/) as path separator as in other Linux-based file locations. (This might lead to failure in managing Apache server installed on the Windows machines).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Apache (Linux) Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Linux** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Apache** radio button.
***Server name**	Enter the name of the designated Linux server.
***IP address/ FQDN**	Enter the IP address of the Apache Server or its fully qualified domain name (FQDN) that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the Apache server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.

   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - AppViewX* • *SSH* **Note:** • If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. (The field label changes to ***Account Name** if **SSM** is the communication mode)
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Access Elevation**	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/ dzdo.
File Upload Temp Path	This field is displayed when the *Access Elevation* = *sudo or dzdo*. Enter the temporary directory/path where certificates or keys are stored during certificate push actions. *Example*: /tmp/files **Note:** It is used as an intermediate location to store the actual keystore and then perform actions on the certificates in the keystore. The keystore is then moved back to the original location after performing the actions.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
Account number	Enter the 12-digit AWS account number. *Example*: 012345678901

8. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the actual directory/path where certificates are stored in the Apache server. *Example*: /cert/files
Key location	Enter the actual directory/path where keys are stored in the Apache server. *Example*: /key/files
Intermediate location	Enter the temporary or intermediate directory/path where certificates and keys are stored in the Apache server. *Example*: /inter/files

9. Click **Add**.
   Once the server is added successfully, the certificate location will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
11. Click **Save**.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.
- If you want to troubleshoot apache linux, see Troubleshooting Apache Linux.

Apache (Windows)

Prerequisites

1. Ensure that application/service users have the appropriate read/write permission to perform the CLM actions on the server device, if the access elevation is selected as **None**.
   When the access elevation is **sudo** or **dzdo**, all the commands used to perform the CLM operations will be executed with sudo or dzdo.
2. Verify that the commands needing sudo or dzdo access have been enabled on the server.
3. Ensure that the following packages are installed to facilitate device addition:
   - sudo/dzdo (optional, as per the access elevation selected)
   - timeout
   - base64
4. Ensure that the target IP address is accessible from the cloud connector and the port is open.
5. Make sure that the language setting for the Apache Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
6. Only certifiticates in .pem, .crt, and .cer formats and key files are discovered.
7. SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
8. Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Verify the existence of **httpd.conf** file in the system by scanning from root directory. Use the command: find / -name “httpd.conf”.
10. Check for the ServerRoot location in the **httpd** file. Make sure it holds forward slashes(/) as path separator as in other Linux-based file locations. (This might lead to failure in managing Apache server installed on the Windows machines).

Onboarding Apache (Windows) Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Microsoft** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Apache** radio button.
***Server name**	Enter the name of the designated Apache server.
***Hostname**	Enter the hostname of the Apache Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Apache server. Gateway is the preferred communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - AppViewX **Note:** If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
*: Mandatory fields	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

8. Enter the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • **Remote** **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	From the following options, select the gateway: • New • Existing
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

9. Click **Save**.
   The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.
- If you want to troubleshoot apache windows, see Troubleshooting Windows Apache Server.

Arbor

Onboarding Arbor

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Arbor** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Arbor server to be onboarded.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Arbor server.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Arbor server device.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.

Vendor Specific Details - Field Description Table

Fields	Description
***Base URL**	Enter the base URL where the Arbor service is hosted.
***HSM Username**	Enter the username used to access the HSM device where the SSL/TLS certificates are stored.
***API Token**	Enter the API token to authorize the communication between AppViewX and the Arbor.
***HSM Password**	Enter the secure password used to access the HSM device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

8. Click **Save**.
   The Arbor device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

CISCO

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

CISCO CUCM

For CISCO CUCM, access privileges are needed for executing the CLM commands corresponding to the supported CLM features (discovery, CSR generation, push, and bind).

For executing these commands, ensure that the admin user has an access privilege of level 1 (read and write access)

For links to detailed documentation on the commands and access privileges, see the References section.

CISCO ISE

- Ensure that at least one node is designated as the primary node.

  Cisco ISE can have one primary PAP node and multiple secondary nodes. AppViewX will always discover certificates from the primary node.

  In the absence of a designated primary node, certificates will not be discovered from Cisco ISE.

  If a primary node is designated but is disabled, only trust certificates will be discovered.
- Ensure that the API setting is enabled for both ERS and OpenAPI.

  Cisco ISE recommends to use port 443 for both ERS and OpenAPI.
- Ensure that the onboarding user has been mapped to the ERS Admin group

For links to detailed documentation for ISE installation and configuration, see the References section.

CISCO IOS

For CISCO IOS, access privileges are needed for executing the CLM commands corresponding to the supported CLM features (discovery). Each user is assigned a privilege level between 1 and 15, and each command has an associated level. The privilege level determines what commands a user can execute.

For links to detailed documentation on the commands and access privileges, see the References section.

Onboarding CISCO

The CISCO device can be on-boarded by four server types,

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- UCS
- CUCM
- ISE
- IOS.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **CISCO** logo from the Vendors list.
   The **CISCO** server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

   a. Select the **Server Type = UCS**, and enter the details of the fields mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type from the dropdown (UCS).
***Server name**	Enter the server name, a unique name for the device addition.
***IP address/ FQDN**	Enter the valid IP address or FQDN for device communication and integration with CISCO.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Cisco server.
***SSH Port**	Enter the SSH port number. Default value is 22.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

b. Select the **Server Type = CUCM**. All the fields mentioned above (in step a) will be displayed along with the additional fields as below:

Server Details - Field Description Table

Fields	Description
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

c. Select the **Server Type = ISE**. All the fields mentioned above (in step a) will be displayed along with the additional fields as below:

Server Details - Field Description Table

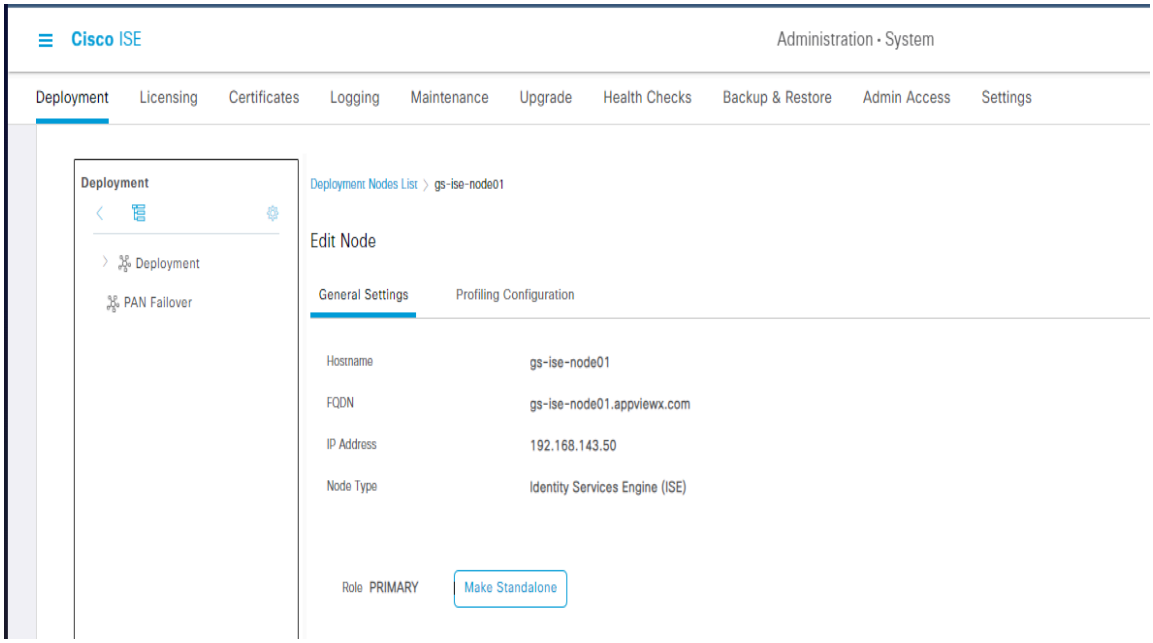
Fields	Description
ERS API Port	The Cisco Identity Services Engine (ISE) API uses ERS and OpenAPI port for communication. These port requirements can be modified during the installation or configuration of the ISE, depending on the network and security requirements. The default value for ERS API Port is **9060**.
Open API Port	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The default value for Open API Port is **443**.
Proxy Required	The checkbox is not selected (false) by default. To enable communication through proxy servers select the checkbox (true).
Cert sync	Select the required cert sync. The possible options are • Managed (*default selection*) • Monitored • Ignored

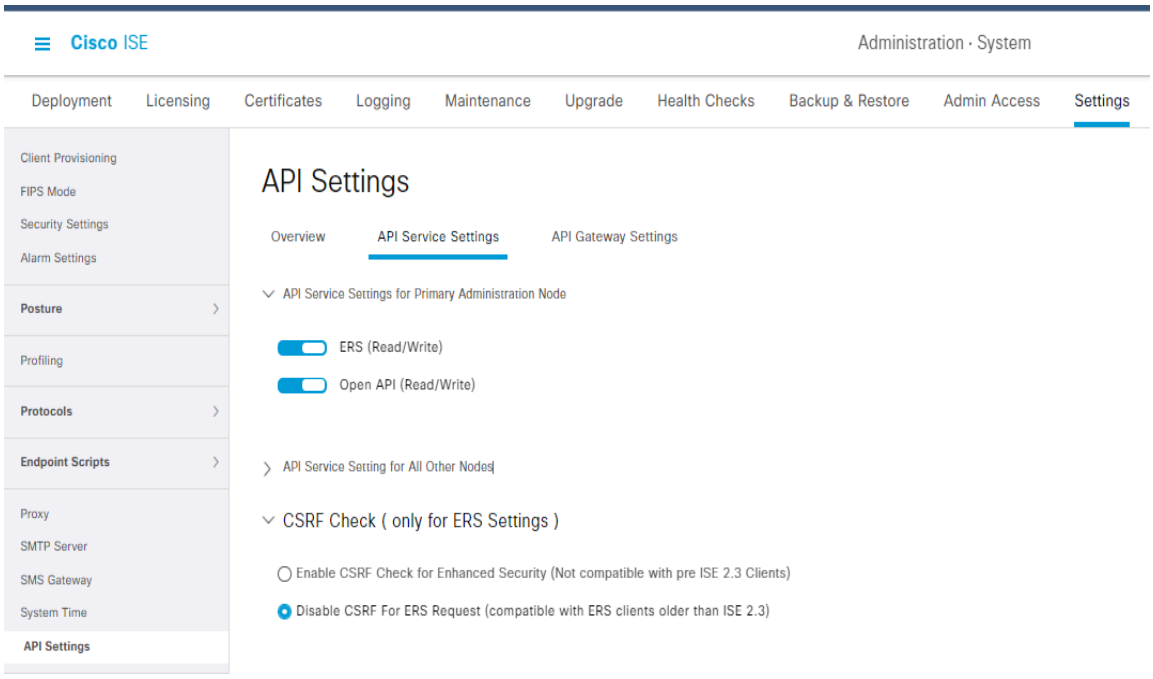
Cisco ISE Device Onbording - Prerequisite

i. Make sure that one of the nodes is designated as the Primary node. If no Primary node is set, server certificates will not be discovered from Cisco ISE. When disabled, only trust certificates will be discovered.



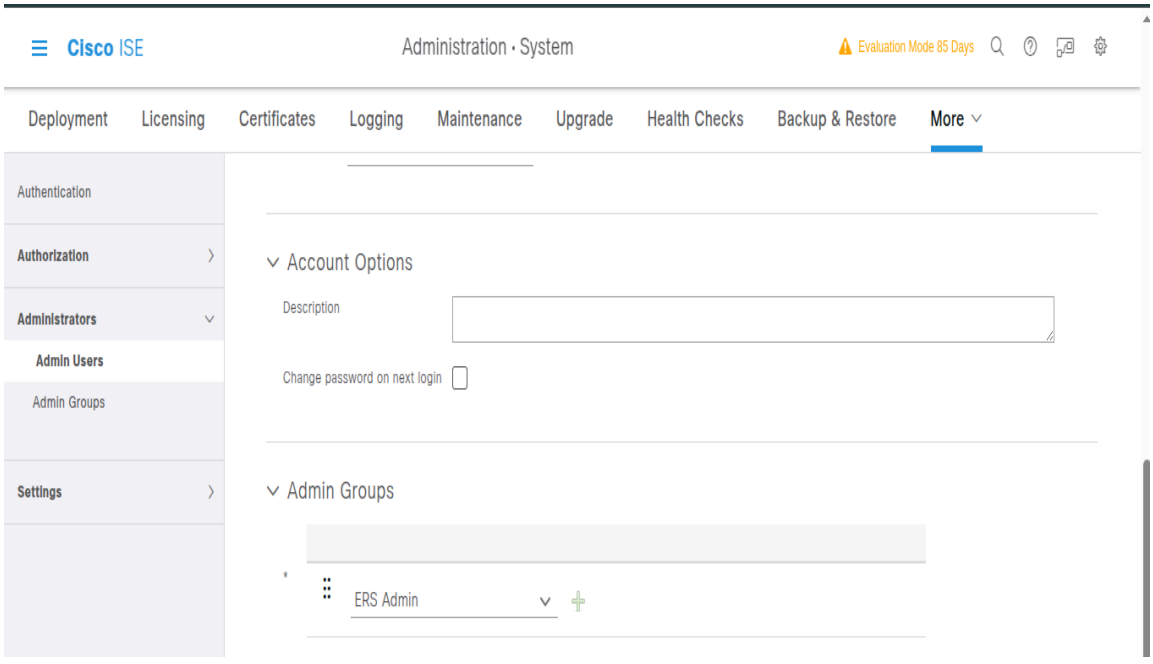
ii. Make sure the API setting is enabled for both ERS and OpenAPI. API services are disabled by default. To enable it, navigate to **Administration** > **System** > **Settings** > **API Settings** > **API Service Settings**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



iii. Cisco ISE recommends to use port 443 for both ERS and OpenAPI.

iv. Make sure the onboarding user has been mapped to the ERS Admin group.



v. Cisco ISE can have one primary PAP node and multiple secondary nodes. AppViewX will always discover certificates from the primary node.

Additional Fields Support for Rest API based vendors

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Additional Fields	Supported in AppViewX
Proxy Required	Yes
The Cisco Identity Services Engine (ISE) API uses ERS and OpenAPI port for communication	
ERS Port	443 or 9060 (External Restful Services)
Open API Port	443

Discovery

i. AppViewX discovers all trust certificates and system certificates from the primary node.
ii. AppViewX would also show the certificate associatation to the role details in the discovery response and also in the app connector.
iii. A profile will be created for the primary node, along with dedicated profiles for each existing certificate.
   - 1. If the profile name follows the format `{deviceName}:{primary_node_name}`, it is used for pushing certificates to Cisco ISE but cannot be used to map certificates to any role.
   2. If the profile name follows the format `{deviceName}:{primary_node_name}:{commaSeparatedRoleName}:{friendlyName}`, the profile can be used to renew, push, and bind the certificate to the specified roles.

Push Format Support

Push Format	Supported in AppViewX
PEM	Privacy Enhanced Mail (PEM)

AppConnector

Field Name	Details
Friendly Name	Enter a friendly name for the certificate. If no name is specified, Cisco ISE automatically creates a name in the format **common-name**, **Subject-Alternative-Name#issuer#nnnnn** where **<nnnnn>** is a unique five-digit number.

i. If the trust certificate already exists in Cisco ISE, pushing it again is not required.
ii. If the admin profile is selected, the application server will restart automatically.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** It is recommended to include both the FQDN and IP address of the ISE server in the SAN field of the ISE system certificate.

iii. The private key is required to push the certificate to Cisco ISE.
iv. If no role or 'Used By' value is defined, the certificate will be pushed to the Cisco ISE system certificate but will remain in a **Not In Use** state.
v. Users cannot uncheck the pre-selected role from the discovered certificate. However, additional roles can be added based on the role selection rules.
vi. During the push process, users can select multiple roles for the certificate, in accordance with the rules defined in Cisco ISE.
vii. The SAML role cannot be combined with any other role.
viii. If the ISE Messaging service role is selected, users should not be allowed to select any other roles from the dropdown.
ix. If the portal role is selected, the **Default Portal Certificate Group** is used as the `portalGroupTag`; custom groups cannot be selected from the AppViewX application.
x. Each role can be associated with only one system certificate. Assigning a new certificate will remove the role from the existing certificate.
xi. Users can utilize the existing configuration to push and bind the certificate.
xii. By default, the use of existing configuration is enabled on the Add/Edit App Connector screen.
xiii. Users can disable the 'Use Existing Configuration' option and provide a new Friendly Name and Roles for the certificate.
xiv. Certificate push operations always upload the certificate to the primary node. Customers must manually transfer the certificate from the primary node to the respective target node.
xv. If the user selects the Node profile to push a new certificate to a role, the existing certificate bound to that role cannot be identified, so a backup cannot be taken. As a result, the backup step will be skipped with the comment: 'No data available,' and rollback will not be possible.
xvi. Cisco ISE does not allow pushing a new certificate with the same public key and will throw the following exception. Therefore, the user must regenerate the certificate before proceeding with the push. Found a certificate with matching public key.

Limitation

- CSR generation at the Cisco ISE endpoint is not supported.

d. Select the **Server Type = IOS**. All the displayed fields are as mentioned in **step b**.

6. In the **Credentials** section, select/enter the details as follows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • Manual entry • Credential List - AppViewX • Credential List - BeyondTrust • Credential List - Thycotic **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the assigned username. (This field is displayed for Manual entry only)
***Password**	Enter the secure password. (This field is displayed for Manual entry only)
***Privilege Password**	Enter the privilege password for using the privilege mode.
**: Mandatory fields*	

7. Click **Save**.

Note: The Cisco device can be configured through the Import option, by downloading the .csv or .xlxs templates, Additional columns (ERS API Port and Open API Port) have been added for Cisco ISE. These can be left blank; the default values, 9060 and 443 respectively will be considered.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

References

- For Cisco CUCM
  - CLI Privilege Levels
- For Cisco ISE
  - Cisco ISE Installation Guide
- For Cisco IOS
  - Cisco IOS Privilege Levels
  - Cisco IOS Configuration Fundamentals Command Reference
  - Controlling Switch Access with Passwords and Privilege Levels

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Dell

Prerequisites

- iDRAC integration is enabled using the Redfish API. Redfish API is enabled by default in most iDRAC9 and iDRAC10 firmware versions. However, if it is disabled or access is restricted, enable it via the iDRAC GUI , navigate to:**iDRAC Settings > Services > Redfish**.
- The onboarding user for iDRAC must have the **Operator** role assigned.
- Verify that the target server's **FQDN** or **IP Address** is reachable from the cloud connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Dell

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Dell** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type has default value **iDRAC** (Integrated Dell Remote Access Controller).
***Server name**	Enter the name of the designated Dell iDRAC server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) of the device being onboarded. It is used for device communication and integration with the server.
HTTPS Port	Use the HTTPS Port enabled in the iDRAC webserver setting. **Note:** Default value is 443.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the SAP server.
Proxy required	To enable communication through proxy servers select the checkbox. **Note:** By default, the checkbox is not selected.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *All supported Internal and external vault* **Note:** If the **Credential Type** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.
***Password**	Enter the secure password.
**: Mandatory fields*	

7. Click **Save**.

   The Dell iDRAC device is onboarded successfully.

Enroll Certificate

Prerequisites and Validation Rules for Endpoint CSR generation:

The following fields are **mandatory** and must be validated:

- Common Name
- Organization

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- City
- State
- Country
- Organizational Unit

Note: All the above fields are required. Missing any field will result in a validation error with a user-friendly message.

Validation Rules

- All the above fields are required. Missing any field should result in a validation error with a user-friendly message.
- Alternative Names:
  - Valid DNS entries.
  - Can only include letters, numbers, and dots (.), and must not contain spaces, underscores (_), or other special characters.
- Common Name, Organization, City, State, and Country must:
  - Only letters, numbers, dots (.), spaces, and underscores (_) are allowed.
  - Other special characters are not permitted.
- Key Type and Size Constraints (iDRAC-specific):
  - iDRAC primarily supports the **RSA** key type.
  - **DSA** and **Elliptic Curve (EC)** key type is not supported
  - By default, iDRAC uses **RSA 2048-bit** keys with **SHA-256** for cryptographic operations.

Discovery Certificate

AppViewX discovers the certificate from the iDRAC SSL/TLS settings and creates the following profiles.

- {deviceName}:@adminPortal
- {deviceName}:@adminPortal:@customSigningCertificate

Note: Private keys cannot be exported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Push Certificate

- Use `{deviceName}:@adminPortal` profile will be used to push both SSL/TLS Certificate Signing Request and SSL/TLS Custom Certificate
- Use the `{deviceName}:@adminPortal:@customSigningCertificate` profile to push only the custom signing certificate. Once pushed, iDRAC will generate a self-signed certificate that is signed using the provided custom signing certificate
- After the certificate is pushed, iDRAC automatically performs a reset. During this process, iDRAC may be temporarily unavailable for a few minutes.

> **Note:** The existing certificate remains active until the reset is completed.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HP-ILO

Onboarding HP-ILO

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select the **HP** logo from the Vendors list.
5. In the **Server details** section, select/enter the details as follows

Server Details - Field Description Table

Fields	Description
***Server Type**	The value is set to ILO.
***Server name**	Enter the name of the designated HP server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.
HTTPS Port	Enter the HTTPS port number used for secure communication.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the HP server.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. Click **Save**.

Note: Multiple devices can be configured for the same vendor.

The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Device Status Log pop-up is displayed.

5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

IBM

Prerequisites

1. Ensure that application/service users have the appropriate read/write permission to perform the CLM actions on the server device, if the access elevation is selected as **None**.
   When the access elevation is **dzdo**, all the commands used to perform the CLM operations will be executed with dzdo.
2. Verify that the commands needing dzdo access have been enabled on the server.
3. [Websphere Linux] Ensure that the following packages are installed to facilitate device addition:
   - dzdo (optional, as per the access elevation selected)
   - SFTP
4. Ensure that the target IP address is accessible from the cloud connector and the port is open.
5. Make sure that the language setting for the Websphere Server is set to English. Ensure that the dzdo prompt string follows the standard Linux format, which is typically "[dzdo] password for <your_username>:"
6. Only certifiticates in p12 and .jks formats and key files are discovered.
7. SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
8. Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Confirm that the WebSphere instance is properly configured with the necessary profiles, servers, and management scope, including the correct cell and node details.
10. Ensure the `security.xml` file is present, the WebSphere server is running, and the user can successfully login to the `wsadmin.sh` script using the required WebSphere wsadmin credentials.

Note: We currently do not support WebSphere management scopes that lack either cell or node information. Please ensure that all management scopes contain this information.

Onboarding WebSphere (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **Websphere (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated websphere server.
***IP address**	Enter the IP address of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - AppViewX • *Credential List* - HashiCorp • *SSH* **Note:** • All other vault settings (BeyondTrust, Cyberark, Hashicorp Vault, Thycotic, and so on.) configured in the **Credentials** will be displayed in the dropdown. • If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If **Credential list - HashiCorp** is selected, the ***Credentials list** dropdown field is displayed with credential type by default. • If SSH is selected, enter the ***Username**, ***Upload key** file, and optionally enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Service account credentials** section, enter the details as indicated below. These credentials are used by the WebSphere application server to perform various tasks, such as accessing files, interacting with the operating system, and communicating with other applications and services.
   If the interactive mode is not enabled for the service account on the Linux machine, the configured service account will switch the session from the logged-in SSH account to the service account using the command: `su - {serviceUserName}`. Once the session is switched, all subsequent commands will execute within the context of the service account session.

   Service account credentials - Field description table

Fields	Description
***Username**	Enter the designated username for authentication.
***Password**	Enter the secure password.
**: Mandatory fields*	

> **Note:** The SSH user, or the service account (if service credentials are enabled), must have read and write access to the WebSphere configuration and cert directory where certificates will be/are deployed.

8. In the **WSadmin credentials** section, enter the details as indicated below. These credentials are used to authenticate the wsadmin tool with the WebSphere Application Server so that it can execute administrative commands and access the necessary resources.
   Irrespective of the SSH user or service account user configuration, **wsadmin** credentials are required for us to open an **interactive administrative scripting session** where we can execute WebSphere management commands. In **WebSphere Application Server (WAS)**, **wsadmin** is the standard and recommended way to manage configurations like SSL, keystores, and bindings — because these changes are part of the **WebSphere configuration repository (config cells, nodes, servers, etc.)**.

   WSadmin credentials - Field description table

Fields	Description
WSadmin User name	The administrative user account for IBM WebSphere Application Server that has the privileges to access and interact with the wsadmin interface.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
WSadmin Password	The password corresponding to the WebSphere administrative user. This account must have permissions to execute wsadmin commands for configuration and management tasks.
WSadmin directory path	The absolute path to the root directory where IBM WebSphere Application Server is installed. This path is required to locate and run the wsadmin tool. **Example path:** /opt/IBM/WebSphere/AppServer/

9. Click **Add**.
   The WSadmin details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the WSadmin details from the list.
11. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *None* • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
Temporary Push Location	Enter the temporary directory/path where certificates or keys are temporarily stored during certificate push actions. If service account credentials are being used, ensure that both the SSH user and Service user have read, write, and execute (RWX) permissions for the specified temporary directory. *Example*: /tmp/files

12. In the **Certificate details** section (optional to discover non-profile certificate), enter the details as indicated below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the java keystore that contains the private key and an associated certificate. *Example*: /tmp/certs/sample.jks
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the java keystore that contains the CA certificates. *Example*: /tmp/certs/sample.jks
Trust store password	Enter the trust store password to access the keystore location.

13. Click **Add**.
    The certificate details are listed in the table.
14. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
15. Click **Save**.
    The device is onboarded successfully.

Websphere (Linux) Commands for CLM Operations

Operation	Command	Description	Dzdo Configuration Required?
Session configuration commands (Executed post creation of ssh session for all use-cases)	bind 'set enable-bracketed-paste off'	Disable the bracketed-paste configuration for the current session	No
	export PS1="bash-4.3~"	Set the ssh session prompt string	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	`uname -a`	To identify the OS details (AIX OS has some changes in the command fomat)	No
PreConfig fetch	ps -eaf|grep 'websphere'"	This would return all the running WebSphere processes in the device.	No
	/opt/IBM/WebSphere/AppServer/bin/versionInfo.sh |grep -w 'Name ' --color=never	To check if the given installation has **IBM WebSphere Application Server** installed.	No
	/opt/IBM/WebSphere/AppServer/bin/versionInfo.sh | grep -w 'Version ' --color=never	This would return the version details of the installed WebSphere instance.	No
Config fetch (For each installation path)	./manageprofiles.sh -listProfiles	This command in WebSphere Application Server is used to display a list of all profiles currently configured on the server	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	./wsadmin.sh -lang jython -user USERNAME -password PASSWORD	Opens an **interactive administrative scripting session** where we can execute WebSphere management commands.	No
	print AdminConfig.list('Security')	Prints the **Security configuration object(s)** currently defined in WebSphere Application Server.	No
	cat /opt/IBM/WebSphere/AppServer/profiles/TestServer01/config/cells/TestCell01/security.xml	Displays the WebSphere Application Server **security configuration XML** for profile TestServer01 and for the cell `TestCell01`. This is required to identify the keystore locations and assist in framing the profile settings.	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Discovery	SFTP Protocol	SFTP is used to retrieve certificates from the keystore location. When the service account is enabled, the certificate is first copied to a temporary directory. After that, the certificate content is fetched using the SFTP protocol.	No
Csr Generation	openssl req -nodes -newkey {keyType}:{bitLength} -{hashFuntion} -days {validityInDays} -keyout {keyFileName}.key -out {csrFileName}.csr -subj '/C={country}/ST={state}/L={location}/O={organisation}/OU={organisationUnit}/CN={commonName}/emailAddress={email}/' -config <location>/{csrConfFileName}	1. RSA as key type To generate csr and key at Websphere endpoint. 2. DSA as key type To generate csr at Websphere endpoint.	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	openssl req -nodes -new -{hashFuntion} -days {validityInDays} -key {keyFileName}.key -out {csrFileName}.csr -subj '/C={country}/ST={state}/ L={location}/O={organisation}/OU={organisationUnit}/ CN={commonName}/emailAddress={email}/' -config <location>/{csrConfFileName}	The command used to generate csr for EC or ECDSA as key type.	No
	openssl dsaparam -out {keyFileName}.key {bitLength}	Command used to generate key at endpoint if key type is dsa	No
	openssl ecparam -name {algorithm} -genkey -noout -out {keyFileName}.key	Command used to generate key at endpoint if key type is ec or ecdsa	No
Push	find /opt/IBM/WebSphere/AppServer -type f -name keytool 2> /dev/null | head -1	Running a command to **find the first occurrence of the** `keytool` **binary** inside the WebSphere installation directory.	No
	Sftp protocol	We will use SFTP to upload the certificate generated by AppViewX to the temporary directory on the target WebSphere device. After	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

		that, we will import the certificate into the target keystore using the keytool command.	
	/opt/IBM/WebSphere/AppServer/ jre_8.0.8010.20230917_1318/jre/bin/keytool -changealias -alias 'cn=appviewx123.test.com, sn=be:1b:39:fc:d1:44:ca:59:b9:c2:00:dd:2e:3b:f7:63' -destalias 'webspheredefaultpush' -storepass appviewx@123 -keystore '/tmp/ appviewx123.test.comBE1B39FCD144CA59B9C200DD2E3BF763.jks'	First, we generate the certificate in AppViewX and upload it to the temporary location. If the user has provided a custom alias name, we then update it using this command. Otherwise, it will have the default alias name framed from the CN	No
	/opt/IBM/WebSphere/AppServer/ jre_8.0.8010.20230917_1318/jre/bin/keytool -importkeystore -noprompt -srckeystore '/tmp// appviewx123.test.comBE1B39FCD144CA59B9C200DD2E3BF763.jks' -destkeystore '/Location/webspheredefaultpush.jks' -srcstorepass appviewx@123 -deststorepass appviewx@123	Copying certificates, private keys, and trusted entries from a source keystore to a destination keystore.	No
	rm -rf	remove temp files	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Bind	"AdminTask.createKeyStore('[-keyStoreName keyStoreName -scopeName managementScopeName -keyStoreType "keyStoreType -keyStoreLocation keyStoreLocation -keyStorePassword keyStorePassword -keyStorePasswordVerify keyStorePassword -keyStoreIsFileBased true -keyStoreInitAtStartup true -keyStoreReadOnly false]')"	The AdminTask.createKeyStore command in WebSphere is used to create a new keystore in the server configuration with specified settings	No
	AdminTask.modifySSLConfig('[-scopeName managementScope -alias storeName -clientKeyAlias " trimmedAliasName -serverKeyAlias trimmedAliasName -keyStoreName keyStoreName -trustStoreName trustStoreName -keyStoreScopeName managementScope -trustStoreScopeName managementScope -securityLevel HIGH]')	The AdminTask.modifySSLConfig command in WebSphere is used to modify the SSL configuration for a specified management scope. This command allows you to set various SSL properties, including keystore and truststore details	No
	print AdminConfig.list('Server')"	The AdminConfig.list('Server') command in WebSphere is used to retrieve a list of all server configuration	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

		objects in the WebSphere Application Server environment. This command provides detailed information about each server, such as its name, type, and associated settings.	
	"AdminTask.modifyKeyStore(' -keyStoreName keyStoreName -keyStoreLocation keyStoreLocation -keyStoreType type -keyStorePassword keyStorePassword'")	The command AdminTask.modifyKeyStore is used in IBM WebSphere Application Server to modify the attributes of an existing key store. A key store is a repository of security certificates and private keys used to establish secure communications.	No
	AdminTask.modifySSLConfigGroup('[-name sslConfigGroupName -direction inbound -certificateAlias trimmedAliasName -scopeName managementScope	The command AdminTask.modifySSLConfigGroup is used in IBM WebSphere	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	-sslConfigAliasName storeName -sslConfigScopeName "managementScope]')	Application Server to modify the settings of an SSL configuration group. SSL configuration groups allow you to manage multiple SSL configurations collectively, making it easier to handle security settings for various applications and services.	
	AdminConfig.save()	The AdminConfig.save() command is used in IBM WebSphere Application Server's administrative scripting environment (wsadmin) to persist any changes made to the configuration.	No
Service Restart	./startServer.sh SERVERNAME	This script, located in the	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

		bin directory of a WebSphere profile, is the utility for starting WebSphere server instances.	
	./stopServer.sh -user USERNAME -password PASSWORD	This script, located in the bin directory of a WebSphere profile, is the utility for stoping WebSphere server instances.	No

Onboarding Websphere (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows:

Server details - Field Description Table

Fields	Description
***Server Type**	Select the **Websphere (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated websphere server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Communication mode	Select *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the IBM Windows server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Apache server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown: • *Manual entry* (default) • *Credential List* - AppViewX • *Credential List* - HashiCorp

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • All other vault settings (BeyondTrust, Cyberark, Hashicorp Vault, Thycotic, and so on.) configured in the **Credentials** will be displayed in the dropdown. • If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If **Credential list - HashiCorp** is selected, the ***Credentials list** dropdown field is displayed with credential type by default.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is displayed only if **Communication mode = Gateway**)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Windows gateway details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value *Remote* is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. In the **WSadmin credentials** section, enter the details as indicated below. These credentials are used to authenticate the wsadmin tool with the WebSphere Application Server so that it can execute administrative commands and access the necessary resources.

WSadmin credentials - Field description table

Fields	Description
***WSadmin User name**	The administrative user account for IBM WebSphere Application Server that has the privileges to access and interact with the wsadmin interface.
***WSadmin Password**	The password corresponding to the WebSphere administrative user. This account must have permissions to execute wsadmin commands for configuration and management tasks

9. Click **Add**.
   The WSadmin details are listed in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. In the **Vendor Specific Details** section, enter the details as indicated below. (This section is displayed only if **Communication mode = SSM**)

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

11. *[Optional]* Click the **Delete** icon, if you want to delete the WSadmin details from the list.
12. In the **Directory** section, enter the details as indicated:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Directory section - Field description table

Fields	Description
WSadmin directory path	The absolute path to the root directory where IBM WebSphere Application Server is installed. This path is required to locate and run the wsadmin tool. **Example path:** C:\IBM_WAS9\WebSphere\AppServer

13. In the **Certificate details** section (optional to discover non-profile certificate), enter the details as indicated:

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the java keystore that contains the private key and an associated certificate. *Example*: C:\keystore\samle.jks
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the java keystore that contains the CA certificates. *Example*: C:\keystore\samle.jks
Trust store password	Enter the trust store password to access the keystore location.

14. Click **Add**.
    The certificate details are listed in the table.
15. *[Optional]* Click the **Delete** icon, if you want to delete the certificate location from the list.
16. Click **Save**.
    The device is onboarded successfully.

Onboarding Data Power

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **Data Power** from the dropdown field.
***Server name**	Enter the name of the designated Data Power server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
***Rest Port**	Retain the value 22; it is the default port used for the communication.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List- Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
Is Https?	Select the checkbox to enable the secure mode.

8. Click **Save**.
   The device is onboarded successfully.

Onboarding Domino

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Server details - Field description table

Fields	Description
***Server Type**	Select the **Domino** from the dropdown field.
***Server name**	Enter the name of the designated domino server.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List- Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory**	Enter the directory/path where the application is installed. *Example*: </Installation_directory/>/domain-registry.xml

8. In the **Windows gateway details** section, enter the details as indicated below.

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Click **Save**.
   The device is onboarded successfully.

Onboarding MQServer (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **MQServer (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated MQServer.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. SSH is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
Region	Enter the geographic region of the AWS instance. *Example*: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

8. Click **Add**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The certificate details are listed in the table.

9. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
10. Click **Save**.

    The device is onboarded successfully.

Onboarding MQServer (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.

   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.

   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **MQServer (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated MQServer.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
Region	Enter the geographic region of the AWS instance. *Example*: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is displayed only when **Communication mode** = **Gateway**).

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

9. Click **Add**.
   The certificate details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
11. Click **Save**.
    The device is onboarded successfully.

Onboarding IBMClient (Linux)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **IBMClient (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated IBMClient server.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

8. Click **Add**.

   The certificate details are listed in the table.
9. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
10. Click **Save**.

    The device is onboarded successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding IBMClient (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **IBMClient (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated IBMClient server.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field description table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below.

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

9. Click **Add**.
   The certificate details are listed in the table.
10. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
11. Click **Save**.
    The device is onboarded successfully.

Onboarding MQClient (Windows)

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **IBM** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server details - Field description table

Fields	Description
***Server Type**	Select the **MQClient (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated MQClient server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the IBM server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the IBM Server that is to be onboarded.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the IBM server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is displayed only when **Communication mode** = **Gateway**).

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway).
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway).
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway).
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway).
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the directory/path where the certificates are stored. *Example*: /etc/pki/java/cacerts

9. Click **Add**.
   The certificate details are listed in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. *(optional step)* Click the delete icon, if you want to delete the certificate location from the list.
11. Click **Save**.
    The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.
- If you want to troubleshoot websphere linux, see Troubleshooting Websphere Linux.
- If you want to troubleshoot websphere windows, see Troubleshooting Websphere Windows.

JBoss

JBOSS can be configured on two types of machines: Linux and Windows. Developed by JBOSS, this server can be deployed on both operating systems, providing flexibility and compatibility for various environments.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

- Ensure that the following packages are installed to facilitate device addition for linux:
  - sudo/dzdo (optional, as per the access elevation selected)
  - timeout
  - base64
- Ensure that the target IP address is accessible from the cloud connector and the port is open.
- Make sure that the language setting for the JBoss Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
- Only certifiticates in .pem, .crt, and .cer formats and key files are discovered.
- SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
- Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.
- Verify that the commands needing sudo or dzdo access have been enabled on the server.
- Check for the ServerRoot location in the **httpd** file. Make sure it holds forward slashes(/) as path separator as in other Linux-based file locations. (This might lead to failure in managing JBoss server installed on the Windows machines).

Onboarding JBoss Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **JBoss** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Operating system type**	Select the **Linux** radio button.
***Server name**	Enter the name of the designated JBoss Linux server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the JBoss server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the JBoss server. **SSH** is the preferred communication mode.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the JBoss server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	By default, application uses none. You can change the command if needed. **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. Click **Save**.
   The JBoss Linux device is onboarded successfully.

Onboarding JBoss Windows

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **JBoss** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Operating system type**	Select the **Windows** radio button.
***Server name**	Enter the name of the designated JBoss Windows server.
***Hostname**	Enter the hostname of the windows server that is to be onboarded.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the JBoss server. **Gateway** is the preferred communication mode.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the JBoss server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the JBoss server device.

   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If the **Communication mode = Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\JBoss-Tomcat-8.5.35
**: Mandatory fields*	

If the **Communication mode = SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\JBoss-Tomcat-8.5.35
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

8. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM**)

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

9. Click **Save**.

   The JBoss Windows device is onboarded successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Generic Linux

Prerequisites

1. Ensure that SSH users have the required read and write permissions to perform CLM actions on the server device when access elevation is set to "**None**."
   If access elevation is configured as "**sudo**" or "**dzdo**," all commands for CLM operations will be executed using sudo or dzdo.
2. If sudo/dzdo access elevation is enabled on the device onboarding page, ensure that the user has the necessary permissions to execute the sudo command provided below.
3. Ensure that the following packages are installed to facilitate device addition:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- sudo/dzdo (Only applicable if access elevation is selected as sudo/dzdo in the device onboarding page)
- timeout
- base64

4. Ensure that the OpenSSL toolkit on the Linux machine is installed.

> **Note:** This package is essential for supporting endpoint enrollment. However, if endpoint enrollment is not required, the package is optional.

5. Ensure the server's resource health remains above the 50% threshold.
6. Ensure that the target IP address is accessible from the cloud connector and the port is open.

> **Note:** To SSH into a machine using a specific port, you can use the following command:
>
> ```
> ssh -p <port_number> <username>@<hostname_or_ip_address>
> ```

7. Ensure that the SFTP is configured.

> **Note:**
> Avoid restricting SFTP sessions to a single connection, as this may cause failures in push use cases. To prevent such issues, adjust the settings in `/etc/security/limits.conf` to allow up to 5 connections.

8. Ensure that GSKit is installed on the server to work with the KDB certificate.
   For the KDB use case, one of the available packages is utilized.

   To verify if the package is installed on the machine, use the following commands:

```
dspmqver -p 64

gsk8capicmd -version | grep FileVersion

gsk8cmd -version | grep FileVersion

gsk7capicmd -version | grep FileVersion

gsk7cmd -version | grep FileVersion
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- The command gsk8capicmd_64 -version will be supported in the future release v2024.2.0.0.
- The first successfully executed command determines the package to be used.

9. To discover a password-protected certificate, ensure the password is added to the password vault at **CERT+** > **ADMINISTRATION** > **Password Vault**.
10. SSH private keys are incompatible with password-enabled sudo/dzdo settings. Therefore, when using an SSH key for authentication, ensure that sudo/dzdo is configured for passwordless access.
11. Certificates cannot be identified from the mounted paths /boot, /bin, /dev, /lib, and /sbin. It is recommended to move the certificate to an alternative location.
12. Host-level configurations take precedence over global settings, allowing you to override global settings at the host level.

Note: The global setting can be configured in the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **(Device Settings)**.

13. Port scanning is disabled by default during Linux discovery. However, configurations are enabled at both the host level and global level to control this feature.
14. If device onboarding fails due to host key algorithm mismatches, activate the required algorithms on the client or server. Add deprecated algorithms only if necessary.
15. It is recommended to exclude the NAS mount paths from certificate scanning which might consume additional resources during scanning and might affect the server performance.

Supported Linux Feature

1. On-demand or scheduled certificate discovery.
2. CSR generation on the end device.
3. Certificate deployment to Linux servers, supporting various certificate types.
4. Delta discovery to identify new or modified certificates.
5. Nightly configuration synchronization job.
6. Authentication via manual entry, SSH, SSM, or external vaults.
7. Service account usage for CLM operations.
8. Global settings for including/excluding file paths in certificate discovery.
9. Configurable port scanning for Linux discovery (disabled by default).
10. Discovery of certificates with case-insensitive file extensions (for example, fileName.kdb or fileName.KDB).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

11. Mapping certificates to specific certificate groups and applying discovery filters.
12. Bulk push support for root and intermediate certificates to one or more devices is now enabled for the Generic Linux vendor.
13. The capability to modify permissions, ownership, group ownership, and other user permissions for pushed certificates is now enabled for Generic Linux in JKS, Keystore, PFX, PEM, and P12 formats.
14. The discovery of extension less trust certificates will be performed if the path is configured with the aggressive scan type during device onboarding. Additionally, the scan will be limited to a maximum depth of 1, and no nested directory scanning will be performed.

Limitations

1. When the same issuer certificate exists in multiple locations, the first one found is prioritized. As a result, even if a renewed certificate is available in another location, only the initial match is considered.
2. In the AIX operating system, identifying certificates located in folders or files with spaces in their names is not supported. However, this functionality is available on non-AIX platforms.
3. The exclusion or inclusion of files using wildcard paths at the global or host level is not supported.
4. Support for elliptic curve (EC) certificates, used in elliptic curve cryptography (ECC), is unavailable in IBM MQ versions prior to version 9.0. This feature is introduced in IBM MQ version 9.0 and later.
5. The push of auto-renewed, regenerated, or discovered password-protected certificates is not supported.
6. App connector cert details cannot be updated when the discovered certificate has a file extension in uppercase.

Onboarding Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select the **Linux** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Linux server that is to be onboarded

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the Linux server.
Data center	Choose the desired data center.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the Linux server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *Credential List - HashiCorp* • *SSH*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • All other vault settings (BeyondTrust, Cyberark, Hashicorp Vault, Thycotic, and so on.) configured in the **Credentials** will be displayed in the dropdown. • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If **Credential list - HashiCorp** is selected, the ***Credentials list** dropdown field is displayed with credential type by default. • If SSH is selected, enter the ***Username**, ***Upload key** file, and optionally enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. **Note:** This field appears when the credential type is selected as Manual entry or SSH.
***Password**	Enter the secure password. **Note:** This field appears when the credential type is selected as Manual entry.
**: Mandatory fields*	

7. In the **Service account credentials** section, select/enter the details as indicated below. If interactive mode is not enabled for the service account on the Linux machine, the configured service account will switch the session from the logged-in SSH account to the service account using the command: `su - {serviceUserName}`. Once the session is switched, all subsequent commands will execute within the context of the service account session.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Service account credentials - Field description table

Fields	Description
Username	Enter the designated username for authentication. **Note:** The service account is not used for authentication; instead, it is used to switch the session from the logged-in SSH user account to the service account.
Password	Enter the secure password.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *None* (default) • *sudo*- to execute with root privileges using sudo access • *dzdo*- to execute with root privileges using dzdo access. **Note:** SSH key-based authentication does not support password-enabled sudo/dzdo.
Discover Formats	The Discover Formats fields contain all the possible certificate formats that are applicable to the 'Default' scan type. The formats include KBD(*.kbd), PEM(*.crt), PEM(*.cer), PEM(*.pem), DER(*.der) DER(*.cer), PKCS#7(*.p7b), PKCS#7(*.p7c), PKCS#12(*.p12), PKCS#12(*.pfx), JKS(*.JKS), JKS(*.keystore). To delete the certificate format from the scan, click the 'x' icon in the respective cert type. To delete all the certificate formats from the scan, click 'Clear' on the top-right of the field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
File Upload Temp Path	This field is displayed if the Access elevation value is selected as sudo or dzdo. Enter the path of the temp folder *Example*: /cert/temp This field is applicable for Push and CSR generation operations. This directory must have common access (RW) for the logged-in user and the service admin user if Service Account credentials are entered.
Enable access elevation for the service account?	When enabled, the commands are executed with selected access elevation. **Note:** • By default, this field is disabled. • This field is enabled only for a service account user when an Access Elevation type, such as sudo or dzdo, is selected.
Enable Network Scan	Select the checkbox to perform a network scan in addition to the managed device discovery scan for these devices. **Note:** • By default, this field is disabled and can be enabled through a global device setting. [**CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **(Device Settings)]**
**: Mandatory fields*	

9. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Certificate Directory	Enter the actual directory/path where certificates are stored in the Linux server. *Example*: /cert/files
Scan Type	Select any of the following: • *Default* - System scans for all certificate formats and adds them in the certificate inventory. **Note:** It scans the provided directory and subdirectory as well. • *Aggressive* - System scans for all keystore files with non-standard SSL extensions and also scans for trust certificates from extension less files. **Note:** It scans only the given directory.
***Operation**	Select the value *include* or *exclude* from the dropdown field. It indicates that the specified certificate directory will be included/excluded from the certificate scan process.
**: Mandatory fields*	

10. Click **Add**.
    The certificate location will be listed in the table.
11. *(optional step)* Click the (Delete) icon if you want to delete the certificate details from the list.
12. Click **Save**.
    The Linux device is added successfully.

Device Settings

Configuring a Global Device setting requires specifying certificate paths to include or exclude from Device Certificate Discovery and Config Sync operations. When enabled for Linux servers, these settings are applied to all added Linux servers.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the ( ) device settings icon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Device Settings** page opens.

4. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate Directory	Enter the actual directory/path where certificates are stored in the Linux server. *Example*: /cert/files
Scan Type	Select any of the following: • *Default* - System scans for all certificate formats and adds them in the certificate inventory. • *Aggressive* - System scans for all keystore files with non-standard SSL extensions.
***Operation**	Select the value *include* or *exclude* from the dropdown field. It indicates that the specified certificate directory will be included/excluded from the certificate scan process.
**: Mandatory fields*	

5. Click **Add**.

The certificate location will be listed in the table.

6. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
7. In the **Vendor Specific details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Enable Network Scan	Enable this checkbox to perform Network Scan along with Managed Device Discovery Scan for these devices.
Certificate Ownership & Permission	Enable the toggle button to customize certificate ownership and file permissions at the App Connector level.
**: Mandatory fields*	

8. Click **Save**.

The Linux device is added successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fetch Config

A prerequisite check evaluates the server's health. If the server is deemed unhealthy, the device is marked as unresolved, blocking discovery for healthy devices. The check monitors average server idle CPU usage, and if it falls below 50%, the sync fails, and the device is marked as unmanaged.

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Select the device from the list to trigger fetch config.
3. Click the (

) **Fetch Config** icon.
   The pop-up message is displayed as **Fitch config has been triggered for the device (s)**.
4. To override the default threshold value, execute the following script in the "cert_metadata" collection.

```
db.getCollection('cert_metadata').updateOne(
{ "_id" : "SERVER_HEALTH_CHECK_CAP"},{ $set:{
    "_id" : "SERVER_HEALTH_CHECK_CAP",
    "map" : {
        "LinuxServer" : "50"
    }
}},{upsert: true})
```

CSR Generation at the End Device

In the CSR generation use case at the end device, the private key will be generated directly on the device. When the private key is generated on the device, the "Private Key at End Device" checkbox will be automatically set to true, and the "Private Key Location" field will be pre-filled in the push app connector.

Certificate Push

1. The Linux push operation allows certificates to be pushed to the Linux server.
   - KDB
   - CRT
   - CER
   - PEM
   - DER
   - P7B

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- P7C
- P12
- PFX
- JKS
- Keystore.

2. For JKS, PEM, and PKCS12 certificates, the capability to modify Certificate Ownership and Permissions after the certificate is pushed has been introduced. This feature is disabled by default and can be enabled by navigating to: **CERT+** > **Device Management** > **Server** > **Device Settings**.
3. If no specific permissions are configured, the pushed certificate will default to 640 permissions. If the file already exists, its existing permissions will be retained.

Possible Error Messages with Linux CLM Use-case

Communication to 192.168.143.30 has failed. Caused by: net.schmizz.sshj.userauth.UserAuthException: Exhausted available authentication methods.	Authentication failure. Check the credentials used for the authentication.
java.lang.Exception: No agent is available as all registered agents are either paused, rejected or deleted or agent resource limit exceeded.	The possible reason(s) could be CC is down or busy processing the other request.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable. Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Device prerequisite check failed: -bash: sudo: command not found. Install the necessary packages (base64, timeout, sudo) to on-board the Server.	The base64, timeout, and sudo packages are required to proceed to onboard the Linux server into AppViewX.
Beyond trust vault response parsing failed:: ["Managed Account not found"].	Verify that the Linux device hostname or IP address is configured for the user in BeyondTrust.
Thycotic vault access token denied / not generated.	Verify the Thycotic vault integration with AppViewX.
No matching password object was found for the query. Ensure a password object exists in the Vault that meets the query criteria and verify that	Verify the Thycotic vault integration with AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

both the Provider and the application user have the necessary permissions to access and use the password.	
CredentialStore(s) does not exist.	Verify that the Linux device hostname or IP address is configured for the user on the Thycotic server.

Linux Commands

Operation	Command	Description	Sudo/Dzdo Configuration Required
Session configuration commands (Executed post-creation of ssh session for all use cases)	bind 'set enable-bracketed-paste off'	Disable the bracketed-paste configuration for the current session.	No
	ulimit -s unlimited	This would set the stack size limit to unlimited for the current shell session or user.	No
	export SUDO_PROMPT='[sudo] password for %p: '	Set the sudo password prompt to the standard value for the current session. **Note:** This will be executed only when the access elevation is set as sudo or dzdo.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	export LANG=en_US.UTF-8	Defaulting the session language to English	
Config fetch	su - {serviceAccountUserName}	Switch to the service account	Yes
	• timeout --version • sudo --version (Optional, based on the access elevation defined in the device onboarding page) • base64 --version	Mandatory package availability prerequisite verification.	No
	uname	To fetch the OS Name	No
	sudo sar 2 5 | tail -1 | awk {'print $NF'}	Server health check for **Linux**	Yes
	sudo sar 2 5 | tail -1 | awk {'print $5'}	Server health check for **AIX** OS	Yes
Discovery	Timeout 120 sudo find <discovery_path> (-path */AvxTempCertDiscovery -prune) -o -type f -iname '*.kdb' 2> /dev/	Find command to identify the KDB Certificates with its checksum.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	null | xargs timeout 120 sudo cksum 2> /dev/null	**Note:** This will be executed only when the KDB cert type is selected	
	• dspmqver -p 64 • gsk8capicmd -version | grep FileVersion • gsk8cmd -version | grep FileVersion • gsk7capicmd -version | grep FileVersion • gsk7cmd -version | grep FileVersion.	The toolkit version is retrieved based on a specified order of preference. Once a version is identified from one of the toolkits, subsequent commands in the sequence are not executed.	Yes
	sudo <toolkit> -cert -list -db <key_database_path> -stashed	List certificates in a specified Key Database (KDB).	Yes
	sudo <kdbtoolkit> -cert -export -db <key_database_path> -stashed -type cms -target_type pkcs12 -target /root/ LinuxServerAvxTempCertDiscovery_1693815850667/ click1602636522.p12 -target_pw #####	Convert KDB certs into p12	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	sudo find '<scan_directory>' -type d 2 > /dev/null -printf "%d\n" | sort -nr | head -n 1	To identify the depth of the directory. Depth search is not available in AIX.	Yes
	Timeout 120 sudo find /<directory> -mindepth 5 -maxdepth 8 \(-path */*AvxTempCertDiscovery* -prune \) -o -type f -iname '*.crt' -o -iname '*.cer' -o -iname '*.p7c' -o -iname '*.p7b' -o -iname '*.key' -o -iname '*.jks' -o -iname '*.pem' -o -iname '*.pfx' -o -iname '*.der' -o -iname '*.p12' -o -iname '.keystore' -o -iname '*.keystore' 2> /dev/null | xargs timeout 120 sudo cksum 2> /dev/null	Use the command to identify a file's path along with its checksum.	Yes
	output="["; for a in '/opt/enrollrabitmq.key' ; do value=$(sudo base64 "$a" 2>/dev/null | tr -d '\n\r'); if [-z "$value"]; then error=$(sudo base64 "$a" 2>&1 >/dev/null); output="${output} {\"file\":\"$a\", \"error\": \"$error\" },"; else	Download cert content from the Linux server in base64 format.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	output="${output} {\"file \":\"$a\", \"value\": \"$value\" },"; fi done; output=${output%,}; output="${output}]"; echo "$output"		
	for p in sudo netstat -anlt | grep tcp | awk -F " " '{print $4}' | awk -F ":" '{print $NF}' | sort | uniq ;do echo "port: $p"; timeout 5 openssl s_client -showcerts -servername server -connect localhost:$p < /dev/null;echo "exit status $?"; done	Network scan	Yes
Temp directory when sudo or service account is used. **Note:** This is used during the CSR generation at endpoint and push operation.	sudo mkdir -p {temp_directory}	Create temp directory	Yes
	chmod 700 {temp_directory} && setfacl -m u:appviewx:rwx -m u:serviceUserName:rwx {temp_directory} **AIX OS Specific Command**: chmod 700 {temp_directory} && (aclget	To address security concerns raised by AppViewX EIS regarding 777 permissions, we are leveraging ACL commands to grant access to both the SSH/SFTP user and the service account user for the temp directory.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	{temp_directory}; echo -e "extended permissions: \nenabled\npermit rwx u:sshUserName \npermit rwx u:serviceUserName") | aclput {temp_directory}	This ensures secure access while allowing uploaded files in the temp directory to be copied to the configured target location. **Note:** The service account username will only be used when the service account is enabled for device onboarding. As a fallback for any failure in executing this command, chmod 777 is applied to the temporary directory created by AppViewX. Once the transaction is complete, the temporary folder is deleted.	
	sudo cp /{temp_directory}/csr_1700139913719.cnf /home/appviewx/	From the temp directory, the uploaded files will be copied to the configured target location.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	sudo rm -rf /{temp_directory}	Remove the temp directory which is created by AppViewX.	Yes
CSR Generation at endpoint	sudo openssl req -nodes -newkey rsa:2048 -sha256 -days 366 -keyout /home/appviewx/report.key -out /home/appviewx/report.csr -subj '/C=/ST=/L=/O=/OU=/CN=report.appviewx.com/emailAddress=/' -config /home/appviewx//csr_1700139913719.cnf	Generating a Certificate Signing Request (CSR)	Yes
Push Cert	sudo find /home/appviewx/devtestcsrgen.keysudo find /home/appviewx -type f -name 'devtestcsrgenkeystore.jkssudo find /home/appviewx -type f -name 'devtestcsrgentruststore.jks'	Verify that the certificate is already present in the target location. If the "Private Key at Endpoint" option is selected and the key does not exist at the specified location, the push operation will fail.	Yes
	sudo stat -c \"%a \" /home/appviewx/existingkeystore.jks sudo stat -c \"%U:%G \" /home/appviewx/existingkeystore.jks	Commands to retrieve the permission and user and user group of the existing Keystore.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(continued)

Operation	Command	Description	Sudo/Dzdo Configuration Required
	sudo mkdir -p {push_path} ; sudo touch {push_path}	Verify if the target directory is editable.	Yes
	sudo echo $HOME	Identify the Home directory	Yes
	sudo openssl pkey -pubout -in /home/appviewx/devtestcsrgen.key | openssl md5	Cert And Key Compatibility Check	Yes
	sudo test -e /home/appviewx/report.pem && echo file exist || echo file not exist	Verify that the certificates already exist in the target location.	Yes
	sudo cp -f '/home/appviewx/devtestcsrgen.key' '/home/appviewx/avx_cert_backup//devtestcsrgen_20230908132855.key'	Take backup if the cert already exists with the same name.	Yes
	sudo openssl pkcs12 -export -in '/home/appviewx/avx.pem' -inkey '/home/appviewx/devtestcsrgen.key' -out '/home/appviewx/p12pushtolinux.p12' -passout ##### -name 'p12pushtolinux'	Export command in case of p12 push.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sudo-enabled Commands

When sudo is enabled, "sudo" is prefixed to all the command executions listed below.

- su
- sar
- find
- mkdir
- netstat **(only if port Scan is enabled)**
- chmod
- chgrp
- chown
- openssl
- base64
- rm
- mv
- touch
- echo
- test
- cp
- cksum
- stat
- setfacl
- "runmqakm", "gsk8capicmd", "gsk8cmd", "gsk7capicmd", "gsk7cmd" , “dspmqver“ **(only if .kdb certs are required, depending on the tool kit currently installed)**.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The **Server Inventory** page is displayed.
3. Check that the device name appears in the inventory (name column) with the specified Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Device Status Log pop-up is displayed.

5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Microsoft IIS

The Microsoft IIS (Internet Information Services) server is a web server developed by Microsoft. It is used to host and serve web applications and websites on Windows Server operating systems. In a typical deployment, an IIS server device is configured with SSL/TLS certificates to secure communications and establish trust between the server and its clients.

Prerequisites

- Both the Windows gateway agent and the windows machine running Microsoft IIS must have administrative privileges.
- Ensure that PowerShell and WinRM tools are installed and running on the Windows machine.
- Verify that Microsoft IIS services are active on the Windows machine.
- At least one website must be configured on the Microsoft IIS server.
- If the Gateway type is selected as WMI, ensure that WMI is properly configured (optional).
- The user must have **read and write permissions** for the folder specified as the **discovery path** and the **push location**.
- The user must have the right **access permissions** to the drive, and the drive must be **configured in sharing mode** to allow discovery and push operations.
- To discover and push the certificate to the store, user should have **Read and write access to the trust store** (to discover and push certificates).

Onboarding Microsoft IIS

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft IIS** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft IIS server.
***Hostname**	Enter the hostname of the Microsoft IIS server that is to be onboarded. **Note:** If the Microsoft IIS server is configured for the integrated Windows Gateway mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Microsoft IIS server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft server device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description

***Credential Type**	Select the credential type from the dropdown.
	• *Manual entry* (default)
	• *Credential List - Appviewx*
	• *Gateway credential*
	• All supported external vaults
	
	Note:
	• If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
	• If **Gateway credential** is selected no other fields are displayed.
	• AppViewX supports the following external credential types:
	  • HashiCorp
	  • CyberArk
	  • BeyondTrust
	  • Thycotic

Certificate Location Details	By default, only the **Certificate store** option is selected for certificate discovery. If the user wants to discover certificates from the **Centralized file system**, they must select the corresponding checkbox, specify the certificate location. The certificate location supports both a shared path and a local file system directory; however, only one of these can be configured at a time. From the given location `pfx and p12 certificates will be discovered.` Choose a pre-configured password vault from the dropdown menu to parse the password protected certificates.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. Enter/Select the **Windows gateway details**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Gateway location**	From the following options, select the gateway location: • Remote • LocalSystem **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***FQDN**	**Note:** This field is displayed when **Gateway location** = **LocalSystem**. Enter the FQDN of the local system on which the Windows Gateway Agent will be installed.
***Port**	**Note:** This field is displayed when **Gateway location** = **LocalSystem**. Enter the port number of the local system on which the Windows Gateway Agent will be installed.
***Select gateway**	**Note:** This field is not displayed when **Windows Gateway Mode** = **Integrated**. From the following options, select the gateway: • New • Existing
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

Microsoft IIS Discovery

The discovery process for Microsoft IIS can leverage multiple sources, as outlined below:

- **File System Discovery**: Requires at least one file path to be specified during device addition.
- **Microsoft Certificate Store Discovery**: Automatically scans the server's certificate store for available certificates.
- **Shared Network Path Discovery:**IIS supports discovery through shared network paths. This means that within the network of the managed IIS device, the logged-in user can be granted access to a shared folder on another system. By specifying that shared network path in the certificate location, the discovery process can be performed successfully.

The **AppConnector** is created dynamically based on the discovery method used.

Connector Behavior for IIS

For certificates discovered from the File System in Microsoft IIS, both Push-only/Default connectors and detailed profile connectors are created. The available profiles depend on the selected push certificate type in the application connector.

Push Certificate Type Options

When adding or updating certificates in Microsoft IIS using the app connector, users can select the desired Push Certificate Type:

a. **Push Certificate:** You can only push certificates to the Certificate store or Centralized File System.
   - Only the Device Name profile is displayed for selection.
   - Profile naming convention:

     `{device_name}`

b. **Push and Bind Certificate:** You can push a certificate to the Certificate store and bind it to the IIS site.

   All detailed profile connectors are displayed for selection, using the convention described below:

   `MS IIS::<siteName>::<host/IP>:<port>:<hostname (optional)>:CS[:(SNI or protocol)]`

   - `<siteName>`: IIS site name or wildcard (*)
   - `<host/IP>`: Hostname or IP address, or *
   - `<port>`: Port number (e.g., 80, 443)
   - `<hostname (optional)>`: FQDN or specific hostname, if applicable
   - `CS`: Certificate Store indicator
   - `:(SNI or protocol)`: *(SNI)* if SNI enabled, *(http)* for HTTP profile, as applicable

   Examples:

   - `MS IIS::test:*:8090:CS`
   - `MS IIS::test:*:443:CS`

Copyright © 2025 AppViewX Inc. All Rights Reserved.

8. In the **Certificate location details** section, enter the details as indicated below.

Certificate Location Details - Field Description Table

Fields	Description
***Location type**	Select to the checkbox for *Certificate store* or *Centralized file system* or both as the location type.
***Certificate location**	Enter the directory or path where the certificate is stored. *Example*: C:\Cert\folder
***Password vault**	Select any of the preconfigured password vault values. None is selected by default.
**: Mandatory fields*	

9. In the **Folder credential details** section, enter the details as indicated below.

Folder Credential Details - Field Description Table

Fields	Description
***Folder credentials**	Select from • Use gateway credential • New • Use device credential (disabled by default)
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *Credential List - CyberArk* • *Credential List - Thycotic* • *Credential List - Hashicorp* • *Credential List - BeyondTrust* **Note:** If **Credential list - Appviewx** or **Credential list - CyberArk** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

10. Click **Save**.
    The Microsoft IIS device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Microsoft PC

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Microsoft PC

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft PC** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft PC server.
***Hostname**	Enter the hostname of the Microsoft PC server that is to be onboarded. **Note:** If the Microsoft PC server is configured for the integrated Windows Gateway mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Microsoft server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft server device.

Credentials - Field Description Table

Fields	Description
Credential Type	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
Username	Enter the designated username for authentication.. (field displayed for manual entry only)
Password	Enter the secure password. (field displayed for manual entry only)

7. Enter/Select the **Windows gateway details**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. Click **Save**.
   The Microsoft PC device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Device Status Log pop-up is displayed.

5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Microsoft Server

Prerequisites

- You must be a local admin user
- You must have **read and write permissions** for the folder specified as the **discovery path** and the **push location**.
- You must have the **access permissions** to the drive, and the drive must be **configured in sharing mode** to allow discovery and push operations.
- You must have **Read and write access to the trust store** to discover and push certificates to the store,.
- If the Gateway type is selected as WMI, ensure that WMI is properly configured.
- The **iisreset.exe** file is expected at the default location. (C:\Windows\System32) to support IIS Service restart

Microsoft Server Discovery

The discovery process for Microsoft servers can leverage multiple sources as outlined:

- **File System Discovery**: Requires at least one file path to be specified during device addition.
- **Microsoft Certificate Store Discovery**: Automatically scans the server's certificate store for available certificates.
- **Port Scan Discovery**: Identifies certificates by scanning specified ports on the server.

The **AppConnector** is created dynamically based on the discovery method used.

Connector Behavior

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- For certificates discovered from the **File System**, a **Push-only/Default Connector** is created by default.
- Profile Naming Convention:
  - deviceName
  - deviceName::StoreName
- You can only push certificates to the Certificate store or Centralized File System.
- If the customer wants to perform **custom operations** (such as validations, service-related activities, backup, etc) **before the push** or **after a successful push operation**, they need to configure and use the **Pre-Script** and **Post-Script Execution** options.
- One or more Store profiles can be selected to push the certificate to the respective store.

Custom Certificate Order for Microsoft Server (PEM Format Push)

When pushing certificates in the **PEM** format to a Microsoft Server, the certificate chain order is controlled through metadata stored in the database.

1. The default format is server:inter:root.
2. If a non-standard certificate order is required, this can be enabled and defined via metadata:

```
db.cert_metadata.update({_id:"CERT_VENDOR_BASED_CONDITIONS"},{"$set": {"map.server_microsoft_server_push_certificate_order" :
"server:root:inter"}})
```

Supported Certificate types for File System Push

- JKS
- Default JKS (creates the JKS file with default password ***changeit*** in the Catalina basepath)
- PEM (*.pem, *.cer and *.crt)
- DER (*.der and *.cer)
- PKCS#12 (*.p12 and &.pfx)
- PKCS#7 (*.p7b and *.p7c)

Onboarding Microsoft Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the ADC tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The Device details page is displayed.
4. Select **Microsoft Server** logo from the Vendors list. The following screen is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. In the **Server Details** section button, enter details as mentioned below.

Server Details - Fields Description Table

Field Name	Description
Server Type	Select Server Type as **Microsoft Server**.
***Server name**	Enter the name of the designated Microsoft server.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Apache server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Microsoft server. Gateway is the preferred communication mode.
Host name	Enter the hostname of the server to be onboarded. **Note:** If the Microsoft Server is configured for the **integrated** Windows Gateway mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as follows.

   If **Communication mode** = **Gateway** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list. • Manual entry • Gateway credentials • Credential List - AppViewX AppViewX also supports the following external credential types: • HashiCorp • CyberArk • BeyondTrust • Thycotic If **Communication mode** = **SSM**, then **Credential list - cloudAccount** is supported.
***Username**	This field is displayed only if **Credential Type** = **Manual Entry**. Enter the username for authentication. **Note:** The username must be added with the domain in the following format: <username>@<domain>.
***Password**	This field is displayed only if **Credential Type** = **Manual Entry**. Enter the password for authentication.
***Credential List**	This field is displayed only if **Credential Type** = **Credential List - AppViewX**. Select the configured credentials value or Default from the dropdown list.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Gateway credentials • Credential List - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext **Note:** Click the (**Settings**) icon next to the field to configure the ARN Advanced Settings.
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Name	Description
	Note: Click the (**Settings**) icon next to the field to configure the S3 Advanced Settings.
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. Enter the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, select/enter the details as follows.

   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Services**	Select checkbox values as **MS Server**, or **Exchange Server**, or **Windows Gateway** or all. The default value is **MS Server**. **Note:** • Selecting all of the services will discover the certificates from MS Server, Exchange Server, and Windows Gateway. • If no services are selected, the service implementation will default to MSServer and CSR generation will be disabled. • The **Exchange Server** option is not supported for **Windows Gateway Mode** = **Integrated** and **SSM**. • Windows Gateway service can be used to enable the CLM support for the Windows GW certificate.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Services**	For SSM the default services enabled is **MS Server**. (Exchange Server is not supported in the cloud).
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance Id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: i-02573cafcftext **Note:** Click the (**Settings**) icon next to the field to configure the ARN Advanced Settings.
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2 **Note:** Click the (**Settings**) icon next to the field to configure the S3 Advanced Settings.
Proxy Required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. In the **Certificate details** section, select/enter the details as follows.

Note: The **Certificate details** section will not be displayed if **Communication mode** = **Gateway** and **Services = Exchange Server** (in the Vendor specific details)

Certificate Details - Field Description Table

Fields	Description
***Keystore Credential Type**	Select the type of credential from the dropdown list. • Manual entry • Credential List - Thycotic **Note:** If **Credential list - Thycotic** is selected, the ***Keystore Credential Name** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Certificate location	Enter the directory/path where the application is installed. *Example*: C:\Microsoft\ADFS\
Certificate Password	Enter the certificate password. This field is only displayed for Keystore Credential Type = Manual entry)
**: Mandatory fields*	

10. Click **Add.**
    Once the server is added successfully, the path will be listed in the table.
11. *(optional step)* Click the (Delete) icon, if you want to delete the server path from the list.
12. Click **Save**
    The device is onboarded successfully.

Onboarding ADFS Server

The ADFS server can now be on-boarded into the AppViewX inventory. To onboard the ADFS server,

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the ADC tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The Device details page is displayed.
4. Select **Microsoft Server** logo from the Vendors list. The following screen is displayed.
5. In the **Server Type** radio button, select/enter the details below.

Server Details - Fields Description Table

Field Name	Description
Server Type	Select Server Type as **ADFS Server**.
***Server name**	Enter the name of the designated Microsoft ADFS server.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Microsoft ADFS server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Microsoft server. Gateway is the preferred communication mode. (SSM is disabled by default)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Name	Description
Host name	Enter the hostname
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. (This option is disabled by default). • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials Section - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Gateway credential • Credential List - AppViewX
***Username**	This field is displayed only if **Credential Type** = **Manual Entry**. Enter the username for authentication.
***Password**	This field is displayed only if **Credential Type** = **Manual Entry**. Enter the password for authentication.
***Credential List**	This field is displayed only if **Credential Type** = **Credential List - AppViewX**. Select the configured credentials value or Default from the dropdown list.
**: Mandatory fields*	

7. In the **Windows gateway details** section, select/enter the details as follows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Windows Gateway Details - Field Description Table

Field Name	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. Click **Save**
   The device is onboarded successfully

The ADFS Server device can also be onboarded by the import functionality using the standard .xlxs and .csv templates available.

To onboard the ADFS server into the AppViewX inventory using the import functionality:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
2. Click the **Server** tab.
3. Click the **Import** button. The Import details page is displayed.
4. Click on the **CSV** or **XLSX** icons in the **Uploader Info** section. The sample templates are downloaded and saved at the default file location.
5. Open the CSV or XLSX templates, enter the relevant information for onboarding the ADFS server, and save the file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Ensure all the mandatory and relevant fields are entered in the .csv or .xlsx template.

6. Click the upload icon in the **Import** section, and select the .csv or .xlsx file from the file dialog box. The status of the uploaded file is displayed in the **File Histories** section.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Limitation

CSR enrollment at endpoint is not supported.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Microsoft SQL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Microsoft SQL

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft SQL** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft SQL server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Microsoft SQL server.
***Hostname**	Enter the hostname of the Microsoft SQL server that is to be onboarded. **Note:** If the Microsoft SQL server is configured for the **integrated** Windows Gateway mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Apache server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft SQL server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** The dropdown displays the credential types configured in the Device Credential section. Additionally, AppViewX supports the following external credential types: • HashiCorp • CyberArk • BeyondTrust • Thycotic.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. Enter/Select the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following features: • Server addition using the **import** feature • Endpoint CSR generation
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, enter the details as indicated below. This section is displayed only if **Communication mode** = **SSM**.

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. Click **Save**.
   The Microsoft SQL device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.
- If you want to troubleshoot Microsoft SQL, see Troubleshooting Microsoft SQL Windows.

MySQL

Prerequisites for Onboarding MySQL

- Ensure that the SFTP package is installed to facilitate device addition.
- Confirm that the target IP address is accessible from the AppViewX Cloud Connector and the corresponding port is open.
- Ensure that the language setting for the MySQL server is set to English.
- Ensure that certificates in the config file are configured with accessible paths. If not, modify the file permissions to make them accessible.

  If certificates do not have the requisite permissions, they cannot be identified from the path.
- Verify that the commands necessitating access have been enabled on the server.
- Verify that the MySQL instance is correctly configured with servers and is running.
- Ensure that the my.cnf file is available at the configured location and the user has all required access to it.

Onboarding MySQL

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the + **(Add)** icon.
4. Select **MySQL** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated MySQL server that is to be onboarded
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the MySQL server.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the MySQL server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the MySQL server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the MySQL server device.

   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Config path	Enter the directory/path where configuration files are stored. *Example*: /tmp/files
*: Mandatory fields	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Config path	Enter the directory/path where configuration files are stored. *Example*: /tmp/files
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the actual directory/path where certificates are stored in the Linux server. *Example*: /cert/files
**: Mandatory fields*	

9. Click **Add**.
   The certificate location will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
11. Click **Save**.
    The MySQL device is added successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

NGINX

Onboarding NGINX

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Nginx** (Green N icon) from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Nginx server to be onboarded.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Nginx server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the Nginx server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Nginx server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access • *None* **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

8. Click **Save**.
   The Nginx device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The Server Inventory page is displayed.

3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Oracle

Onboarding WebLogic (Linux)

Prerequisites

1. Ensure that the following packages are installed to facilitate device addition:
   a. dzdo (Optional, as per the access elevation selected)
   b. SFTP
   c. base64
2. Ensure that the target IP is accessible from the cloud connector and that the port is open.
3. Make sure that the language setting for the WebLogic Server is set to English.Ensure that the sudo/dzdo prompt string follows the standard Linux format, which is typically **"[sudo] password for <your_username>:"**
4. SSH private keys cannot be used with password-enabled dzdo settings. Therefore, if an SSH key is used for authentication, ensure that `dzdo` is configured for passwordless operation.
5. Certificates located in paths without the necessary user permissions cannot be identified, so ensure to either place the certificates in configuration files with accessible paths or adjust the file permissions for accessibility.
6. Ensure that the commands requiring sudo/dzdo privileges are enabled on the server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Ensure that the WebLogic instance is properly configured with the necessary profiles, servers, and SSL certificates.
8. Ensure that the `config.xml` file is present, the WebLogic server is running, and the user can log onto the `wlst.sh` script using the required WebLogic credentials.
9. Ensure access to the `wlst.sh` script as it is used across multiple stages of device onboarding and CLM operations. Below are the key use cases:
   - **Vendor Validation**

     The `wlst.sh` script is run to verify the WebLogic installation. A successful launch without errors confirms the vendor setup.

   - **Version Fetch**

     The WebLogic version is retrieved by executing specific commands within the `wlst.sh` script.

   - **Decrypting Domain Credentials**

     To obtain the WebLogic domain username and password, values are decrypted using commands executed within `wlst.sh`.

   - **Certificate Binding**

     During the certificate binding process, a series of commands are executed through `wlst.sh` to bind the server certificate to the target WebLogic server.
10. The SSH user or service account (if configured) must have **execute (`x`) permission** on the path containing `wlst.sh`, as a `cd` (change directory) operation is performed. Even with access elevation is enabled (e.g., sudo or dzdo), the user must have `x` permission since `sudo` or `dzdo` commands cannot be used with the `cd` command. Ensure the user has all necessary minimum access permissions as mentioned in the next step.
11. The OpenSSL toolkit is required for private key and CSR generation at the target device, so ensure to install it on the Linux machine.
12. **Minimum Permission Required**
    - The SSH user or service account (if configured) must have the necessary permissions to access the path containing `wlst.sh`, with or without `sudo` privileges.
    - The user must have read (r) permission for the `config.xml` and `boot.properties` files, as well as their respective directories. Otherwise, elevated access is required.
    - Additionally, the user must have read and write (rw) permissions for the configured keystores and their directories. Otherwise, elevated access is required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The user must have read and write (rw) permissions on the target location to push the keystore. Otherwise, elevated access is required.
- An SFTP connection is set up for the current user, who might not have the necessary access to the service account's directory. It is recommended to choose a File Upload Temp Path in the UI that allows both the current user and the service account user to read and write.

13. Recommended practices to use AppViewX efficiently:
    - **Config.xml Guidelines:**
      - If the configuration file (`config.xml`) lacks sufficient details to determine the protocol and port, AppViewX defaults to the T3 protocol and its standard port.

        To prevent misconfiguration, ensure the following entries are explicitly defined in `config.xml`:

        - Admin server port
        - Administration protocol enabled
        - Protocol type (for example, HTTP, HTTPS) - if applicable
        - Administration port - if applicable
        - Listen address - recommended for clarity and accuracy.
    - **Java Truststore:**
      - Do not customize the password for the default Java truststore, as WebLogic only recognizes the default password: `changeit`.
      - If a custom truststore path is used, it requires running `./wlst.sh` with specific arguments which is not supported by WebLogic.
      - AppViewX supports pushing certificates only to the default Java truststore location: `/java_path/lib/security/cacerts`.
    - **Server Certificate and Keystore Configuration:**
      - For successful client-side authentication, WebLogic validates the `SSLSocketFactory` hostname verifier.
      - When using T3S or HTTPS protocols, the server certificate must include the WebLogic server's fully qualified domain name (FQDN) in either the Common Name (CN) or the Subject Alternative Name (SAN).
      - Store the server certificate, private key, and full certificate chain in a single keystore entry.
      - Maintain a separate truststore for root and intermediate certificates.

To configure WebLogic (Linux) server:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Select **Oracle** logo from the Vendors list.
   The Oracle server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server type**	Select **WebLogic (Linux)** from the dropdown field.
***Server name**	Enter the name of the designated **WebLogic (Linux)** server.
***IP address**	Enter the valid IP address of the server being onboarded.
Data center	Select the desired data center from the dropdown list. It holds all the SSL What can you do next? that is to be retrieved from the server.
***SSH Port**	Enter the SSH port number. By default, 22 is the port used for the SSH communication mode.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown: • *Manual entry* (default) • *Credential List - AppViewX* • *SSH*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential List from the dropdown menu. **Note:** • If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication. • If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Service account credentials**section enter the details as follows.

Service account credentials - Field Description Table

Fields	Description
Username	Enter the designated username for authentication.
Password	Enter the secure password.

8. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
WebLogic Installation directory	Enter the path where the WebLogic domain-registry.xml file is saved. *Example:*/WL_installation_directory/

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Access Elevation**	Select the type of access elevation from the dropdown list. By default, it is None.
File Upload Temp Path	Enter the temporary file upload path. This field is applicable only for push operations and is enabled when access is elevated using **sudo** or **dzdo**. **Note:** This field is enabled if you access elevation as sudo or dzdo.
**: Mandatory fields*	

9. Click **Add**
   The WebLogic Installation directory is added successfully in the table.
10. (Optional) Click the (Delete) icon, if you want to delete the directory location from the table, or add more WebLogic Installation directories.
11. In the **Certificate details** section (required to discover any additional non-profile certificate), enter the details as follows.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the jks keystore in Oracle Linux that contains the private key and an associated certificate. *Example*: /tmp/certs/sample.jks
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the jks trust store in Oracle Linux that contains the CA certificates. *Example*: /tmp/certs/sample.jks
Trust store password	Enter the trust store password to access the keystore location.

12. Click **Add**
    The keystore location is added successfully in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

13. *(optional step)* Click the (Delete) icon, if you want to delete the certificate location from the list, or add more keystore locations.
14. Click **Save**.
    The Oracle WebLogic (Linux) device is on-boarded successfully.

WebLogic (Linux) Commands for CLM Operations

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
Session configuration commands (Executed post creation of ssh session for all use-cases)	`bash`	Used to set the prompt string for the logged-in user	No	-
	`bind 'set enable-bracketed-paste off'`	Disable the bracketed-paste configuration for the current session	No	-
	`export SUDO_PROMPT='[sudo] password for %p: ' ; export LANG=en_US.UTF-8` **Note:** This command is executed only when access elevation is enabled.	Set the sudo password prompt to the standard value for the current session and update the session language as English US	Yes	-
	whoami	Executed to know the logged-in user	No	-
Pre-config fetch	`ps -eaf|grep 'weblogic'|grep -v grep`	This command is used to check if a WebLogic server process is running on the system.	No	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script

	`cd wlst_path`
	eg:
	`cd/home/appviewx/Oracle/Middleware/Oracle_Home/oracle_common/common/bin`
		Change the current directory to the wlst path	Yes	-

	`find -name 'wlst.sh'`	To find the location of the wlst.sh script	Yes	-
	`./wlst.sh`	The wlst.sh script is used to launch WebLogic Scripting Tool (WLST), which is a command-line utility for managing and automating WebLogic Server administration.	Yes	-
	`print version`	This command is used to find the version of the WebLogic server.	-	Yes
	`exit()`	This command is used to close the wlst.sh script.	-	Yes
Config fetch	`cat 'domain-registry-xml_path/domain-registry.xml'`	This command is used to read the contents of domain-registry.xml file.	Yes	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	`cat 'config_xml_path/config.xml'`	This command is used to read the contents of config.xml file	-	Yes
	`cat 'boot_properties_path/boot.properties'`	This command is used to read the contents of boot.propertiesl file	Yes	-
	`service = weblogic.security.internal.SerializedSystemIni.getEncryptionService('"domainPath "')"`	This command is used in WebLogic Scripting Tool (WLST) to retrieve the encryption service for a WebLogic domain	No	Yes
	`encryption = weblogic.security.internal.encryption.ClearOrEncryptedService(service)`	The ClearOrEncryptedService class in WebLogic allows you to handle encrypted values within WebLogic Server. This is typically used for encrypting and decrypting passwords stored in configuration file.	No	Yes
	`encryption.decrypt('encrypted_password')`	In WebLogic Scripting Tool (WLST), the encryption.decrypt() function is	No	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
		used to decrypt an encrypted password stored in WebLogic.		
	`encryption.decrypt('encrypted_username')`	In WebLogic Scripting Tool (WLST), the encryption.decrypt() function is used to decrypt an encrypted username stored in WebLogic.	No	Yes
Tempora Directory Creation (Only for access elevated user)	`<access-elevation> mkdir -p <temporary-directory>`	A temporary folder is created to upload files into the end machine.	Yes	-
	`uname -a`	To check if the OS is AIX.	No	-
	`<access-elevation> chmod 700 <temporary-directory> && <access-elevation> setfacl -m u:<username>:rwx <temporary-directory>`	Modify access for the current session user.	Yes	-
	`<access-elevation> chmod 700 <temporary-directory> && <access-elevation> setfacl -m`	Modify access for the current session user and service account user.	Yes	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	u:<username>:rwx -m u:<SERVICEACCOUNT>:rwx <temporary-directory> sudo chmod 700 '/tmpfileloc//weblogicLinuxPush_1739432147548' && sudo setfacl -m u:appviewx:rwx '/tmpfileloc//weblogicLinuxPush_1739432147548'			
	<access-elevation> chmod 777 <temporary-directory> sudo chmod 777 '/tmpfileloc//weblogicLinuxPush_1739432147548'	Modify the access to rwx for every user for the temporary account only if the above Access fails.	Yes	-
	<access-elevation> rm -rf <temporary-directory> sudo rm -rf /tmpfileloc//weblogicLinuxPush_1739432147548	Remove the temporary folder after the clm operation scope is finished.	Yes	-
Discovery	base64 '/home/appviewx/oracle_cert1.jks'	Read the content of keystore file using base 64 method.	Yes	-
Csr Generation	<access-elevation> mkdir -p <target-file-directory>;	Test if the folder exists; else, create	Yes	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	<access-elevation> touch <target-file-directory>	a folder (both for CSR and key files)		
	<access-elevation> chown $(id -un):$(id -gn) <csr-config-file>	Change ownership to the logged-in user	Yes	-
	openssl req -nodes -newkey {keyType}:{bitLength} -{hashFuntion} -days {validityInDays} -keyout {keyFileName}.key -out {csrFileName}.csr -subj '/C={country}/ST={state}/L={location}/O={organisation}/OU={organisationUnit}/CN={commonName}/emailAddress={email}/' -config <location>/{csrConfFileName}	1. RSA as the key type To generate CSR and key at weblogic endpoint. 2. DSA as the key type To generate CSR at weblogic endpoint.	Yes	-
	openssl req -nodes -new -{hashFuntion} -days {validityInDays} -key {keyFileName}.key -out {csrFileName}.csr -subj '/C={country}/ST={state}/L={location}/O={organisation}/OU={organisationUnit}/CN={commonName}/emailAddress={email}/' -config	This command is used to generate CSR for EC or ECDSA as the key type.	Yes	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	<location>/{csrConfFileName}			
	openssl dsaparam -out {keyFileName}.key {bitLength}	This command is used to generate a key at the endpoint if the key type is DSA.	Yes	-
	openssl ecparam -name {algorithm} -genkey -noout -out {keyFileName}.key	This command is used to generate a key at the endpoint if the key type is ec or ecdsa.	Yes	-
	<access-elevation> base64 <csr-file-path> sudo base64 / home/appviewx/test/testingweblogic.conf	Command executed to fetch CSR generated at end device.	Yes	-
	<access-elevation> chmod 640 <target-key-file-path>	Update the key file access permission to 640.	Yes	-
	<access-elevation> rm -rf <files>	Executed to remove the cnf(csr config) and csr files created at the endpoint.	Yes	-
Push	<access-elevation> stat -c %a <keystore-location>	To fetch the permission of the file if it exists in the server.	Yes	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	<access-elevation> stat -c %U:%G <keystore-location>	To fetch the ownership of the file if it exists in the server	Yes	-
	<access-elevation> cp <temporary-file-path> <target-location>	Copy the file (keystore) from the temporary location to the target location.	Yes	-
	<access-elevation> chmod <permission-received from stat command/600> <target-keystore-file-path>	Update the file access with existing permission or set it to 600	Yes	-
	<access-elevation> rm -f <temp-file>	Remove the temperory file (This command is executed only in case of enrollment of key at end-point).	Yes	-
Bind	date +%s%3N	This command returns the current timestamp in milliseconds.	Yes	-
	perl -MTime::HiRes -e 'printf(\"%.0f\\n\", Time::HiRes::time() *1000)'	This command returns the current timestamp in milliseconds.	Yes	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	./wlst.sh	-	Yes	-
	connect(USERNAME,PASSWORD,LISTENADRESS)	This function in WebLogic Scripting Tool (WLST) is used to establish a connection to a WebLogic Server.	No	Yes
	edit() startEdit()	This commands are used when making configuration changes to the WebLogic domain.	-	Yes
	cd(TARGET_SERVER_PATH)	The cd() command in WLST (WebLogic Scripting Tool) is used to navigate the hierarchical MBean tree of a WebLogic domain.This command moves into the AdminServer MBean, allowing you to view and modify its attributes.	-	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	`cmo.setKeyStores('CustomIdentityAndCustomTrust')`	cmo refers to the Current Management Object, which represents the MBean of the currently navigated configuration. setKeyStores('CustomIdentityAndCustomTrust') sets the keystore type for SSL configuration.	-	Yes
	`cmo.setCustomIdentityKeyStoreFileName(KEYSTORE_ABSOLUTE_PATH)`	This command is used in WebLogic Scripting Tool (WLST) to set the absolute path of the custom identity keystore for a WebLogic Server instance.	-	Yes
	`cmo.setCustomIdentityKeyStorePassPhrase(PASSWORD)`	This command is used in WebLogic Scripting Tool (WLST) to set the password of the custom identity keystore for a WebLogic Server instance.	-	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
	`cmo.setCustomTrustKeyStoreType('jks')`	This command sets the keystore type for SSL configuration.	-	Yes
	`save()`	This command is used to save the configuration changes to WebLogic.	-	Yes
	`cd(PATH_TO_SSL_SERVER)`	This command moves into the AdminServer MBean, allowing you to view and modify its attributes.	-	Yes
	`cmo.setServerPrivateKeyAlias(PRIVATE_KEY_ALIAS_NAME)`	This command is used in WebLogic Scripting Tool (WLST) to specify the alias of the private key inside the identity keystore for a WebLogic Server instance.	-	Yes
	`cmo.set('ServerPrivateKeyPassPhrase',PASSPHRASE)`	This command is used in WebLogic Scripting Tool (WLST) to set the passphrase for the server’s private	-	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description	Sudo/Dzdo Configuration Required?	Executed in wlst Script
		key stored in the custom identity keystore.		
	cmo.setEnabled(true)	This command is used in WebLogic Scripting Tool (WLST) to enable SSL for a WebLogic Server instance.	-	Yes
	activate()	This command is used to commit and apply configuration changes made in the edit session.	-	Yes
	disconnect()	This command closes the WLST session and disconnects from WebLogic Server.	-	Yes
	cmo.getServerPrivateKeyAlias()	This is a getter method used to retrieve the alias of the private key for the server's SSL configuration.This alias refers to a private key entry in the server’s keystore	-	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- All commands referenced here are executed using the latest version. In legacy versions, some commands may differ or may have been introduced only in the most recent release.
- **Limitations**
  - The **P12** extension is not supported for certificate push.
  - Execute permission is required for the `wlst.sh` path as a `cd` operation is performed to access that directory.
  - Currently, the **t3s** protocol is not supported for server connections. Configure the WebLogic server to use the **t3** protocol instead.

Onboarding WebLogic (Windows)

Prerequisites

- The gateway must be installed within the same domain.
- The WebLogic instance on Windows must be up and running.
- Ensure config.xml is available in the domain directory and the user must have access to it.
- To avoid misconfiguration, ensure that the following details are explicitly defined in the `config.xml`:
  - Admin server port
  - Administration protocol enabled
  - Listen address (recommended for clarity and accuracy)

Access Requirements

If the WebLogic Server instance is running under a service account that is not *Local System* or a member of the *Administrators* group:

- **For a Domain Service Account**: Add the account to the Administrators group on the server.
- **For a Built-in Account (e.g., Network Service):** If the service account user cannot be added to the admin group, then use the **Default connector** to push the certificate. You can then use the **post-script execution** to perform the bind operation.

Best Practice Recommendation

If the same issuer certificate is available in multiple paths, then the first find is considered. Hence, it is recommended to maintain the trust certificates in one common location.

To configure WebLogic (Windows) server:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Oracle** logo from the Vendors list.
   The Oracle server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server type**	Select **WebLogic (Windows)** from the dropdown field.
***Server name**	Enter the name of the designated WebLogic (Windows) server.
Communication Mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Oracle server. Gateway is the preferred communication mode.
***Hostname**	Enter the hostname of the Oracle WebLogic (Windows) server that is to be onboarded. This field is not mandatory if Communication mode is SSM.
Data center	Select the desired data center from the dropdown list. It holds all the SSL What can you do next? that is to be retrieved from the server.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown: • *Manual entry* (default) • *Credential List - AppViewX* • If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential List from the dropdown menu. **Note:** • If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown: • *Manual entry* (default) • *Credential List* - cloudAccount • If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential List from the dropdown menu.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values. • If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine. This field is displayed only when Communication mode is SSM.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine. This field is displayed only when Communication mode is SSM.
**: Mandatory fields*	

7. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM**)

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click **Browse** and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

8. In the **Vendor Specific Details** section enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***WebLogic Installation directory**	Enter a directory where domain-registry file is located. *Example:*/WL_installation_directory/domain-registry.xml
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***WebLogic Installation directory**	Enter a directory where domain-registry file is located. *Example:*/WL_installation_directory/domain-registry.xml
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. [Optional] In the **Certificate details** section, enter the details as indicated below.

Note: You can skip this section as it will be deprecated in the next release.

Certificate Details - Field Description Table

Fields	Description
Key store location	Enter the location of the jks keystore in Oracle that contains the private key and an associated certificate. *Example*: C:\keystore\samle.jks
Key store password	Enter the key store password to access the keystore location.
Trust store location	Enter the location of the jks trust store in Oracle that contains the CA certificates. *Example*: C:\keystore\samle.jks
Trust store password	Enter the trust store password to access the keystore location.

10. Click **Add**.
    The keystore location is added successfully in the table.
11. [Optional] Click the **Delete** icon to delete the certificate location from the list, or add more keystore locations.
12. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The Oracle WebLogic (Windows) device is onboarded successfully.

Note:

Limitations

- The **P12** extension is not supported for certificate push.
- Currently, the **t3s** protocol is not supported for server connections. Configure the WebLogic server to use the **t3** protocol instead.

Pushing Certificates

1. There is an option to deliver the certificate to the WebLogic server in the following formats:
   - JKS
   - keystore
2. When you choose the private key on the device, provide the absolute path of the server-generated private key on the UI screen.

Sample Configuration File

Following is a sample configuration file for config.xml:

```
<server>
  <name>AdminServer</name>
  <ssl>
    <name>AdminServer</name>
    <enabled>true</enabled>
    <hostname-verifier xsi:nil="true"></hostname-verifier>
    <hostname-verification-ignored>true</hostname-verification-ignored>
    <export-key-lifespan>500</export-key-lifespan>
    <client-certificate-enforced>false</client-certificate-enforced>
    <listen-port>7002</listen-port>
    <two-way-ssl-enabled>false</two-way-ssl-enabled>
    <server-private-key-alias>ws</server-private-key-alias>
    <server-private-key-pass-phrase-encrypted>{AES256}Y6nGhqZXlUv+76dQt+w5uOqWrQMUxusqPV3kx4nzi7g=</server-private-key-pass-phrase-encrypted>
    <ssl-rejection-logging-enabled>true</ssl-rejection-logging-enabled>
    <inbound-certificate-validation>BuiltinSSLValidationOnly</inbound-certificate-validation>
    <outbound-certificate-validation>BuiltinSSLValidationOnly</outbound-certificate-validation>
    <allow-unencrypted-null-cipher>false</allow-unencrypted-null-cipher>
    <use-server-certs>false</use-server-certs>
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  </ssl>
  <machine>machine_1</machine>
  <listen-port>7001</listen-port>
  <listen-port-enabled>true</listen-port-enabled>
  <listen-address></listen-address>
  <java-compiler>javac</java-compiler>
  <client-cert-proxy-enabled>false</client-cert-proxy-enabled>
  <key-stores>CustomIdentityAndCustomTrust</key-stores>
  <custom-identity-key-store-file-name>/tmp/keystore.jks</custom-identity-key-store-file-name>
  <custom-identity-key-store-type>JKS</custom-identity-key-store-type>

 <custom-identity-key-store-pass-phrase-encrypted>{AES256}uFlgx8fDT9ag2zGtvcOwjR9HUZRvkIGDdEdHGwpZnsQ=</custom-identity-key-store-pass-phra
se-encrypted>
  <custom-trust-key-store-file-name>/tmp/keystore.jks</custom-trust-key-store-file-name>
  <custom-trust-key-store-type>JKS</custom-trust-key-store-type>

 <custom-trust-key-store-pass-phrase-encrypted>{AES256}45ySG867mJorWxBfHpKK0fWmJGT/07oxPKL8/lYBcF8=</custom-trust-key-store-pass-phrase-encry
pted>
  <server-diagnostic-config>
    <wldf-diagnostic-volume>Low</wldf-diagnostic-volume>
  </server-diagnostic-config>
 </server>
```

Probable Error Messages and Causes for WebLogic CLM Use Case

Error message	**Description**
Communication to <ip/fqdn> has failed. Caused by: net.schmizz.sshj.userauth.UserAuthException: Exhausted available authentication methods	Authentication failure. Kindly check the credentials used for the authentication.
Beyond trust vault, response parsing failed::["Managed Account not found"]	Kindly check whether the weblogic device hostname or IP address is configured for the user in the Beyond Trust.
Thycotic vault access token denied or not generated	Check the Thycotic vault integration with AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Password object matching query was not found. Please check that there is a password object that answers your query in the Vault and that both the Provider and the application user have the appropriate permissions needed to use the password	Check the Thycotic vault integration with AppViewX
CredentialStore(s) does not exist.	Kindly check whether the weblogic device hostname or IP address is configured for the user in the Thycotic server.

Onboarding iPlanet

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Oracle** logo from the Vendors list.
   The Oracle server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details section - Field Description Table

Fields	Description
***Server type**	Select **iPlanet** from the dropdown field.
***Server name**	Enter the name of the designated **iPlanet** server.
***IP address**	Enter the valid IP address of the server being onboarded.
Data center	Select the desired data center from the dropdown list. It holds all the SSL What can you do next? that is to be retrieved from the server.
***SSH Port**	Enter the SSH port number. 22 is the default port used for the SSH communication mode.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as follows.

Credentials section - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown: • *Manual entry* (default) • *Credential List - AppViewX* • If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential List from the dropdown menu. **Note:** • If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values. • If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
***WADM User name**	Enter the username for the WADM CLI (Command line interface) utility. WADM defines all the commands that are supported for configuring and administering the server.
***WADM Password**	Enter the password for the WADM CLI utility.
***WADM directory path**	Enter the file location/directory path to where the WADM utility is stored.
*: Mandatory fields	

8. In the **Certificate Details** section enter the details as follows.

Certificate Details- Field Description Table

Fields	Description
Database path	Enter the file location/directory path of the database where the certificates are stored.
Password	Enter the password for the certificates database.

9. Click **Add**
   The database path is added successfully in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the database path from the list, or add more accordingly.
11. Click **Save**.
    The Oracle iPlanet device is on-boarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.
- If you want to troubleshoot WebLogic linux, see Troubleshooting WebLogic Linux.
- If you want to troubleshoot WebLogic windows, see Troubleshooting WebLogic Windows Server.

Other Devices

Onboarding Other Devices

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Other Devices** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	The server type has a fixed value **Other devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Server name**	Enter a unique name of the designated server to be onboarded.
***IP address/ FQDN**	Enter the valid IP address of the device to be onboarded.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the VMware server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

7. Click **Save**.
   The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

RabbitMQ

Onboarding RabbitMQ

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **RabbitMQ** logo from the Vendors list.
   The RabbitMQ server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the server name.
***IP address/ FQDN**	Enter the valid IP address or FQDN
Data center	Select the desired data center from the dropdown list.
Communication mode	Select the required communication mode. The possible options are: • SSH • SSM
***SSH Port**	Enter the SSH port number **Note:** This field is displayed only if the Communication mode selected is SSH.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. This option is **disabled** by default. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Credential List - AppViewX • Credential List - CyberArk • SSH
***Username**	Enter the username.
***Password**	Enter the password.
**: Mandatory fields*	

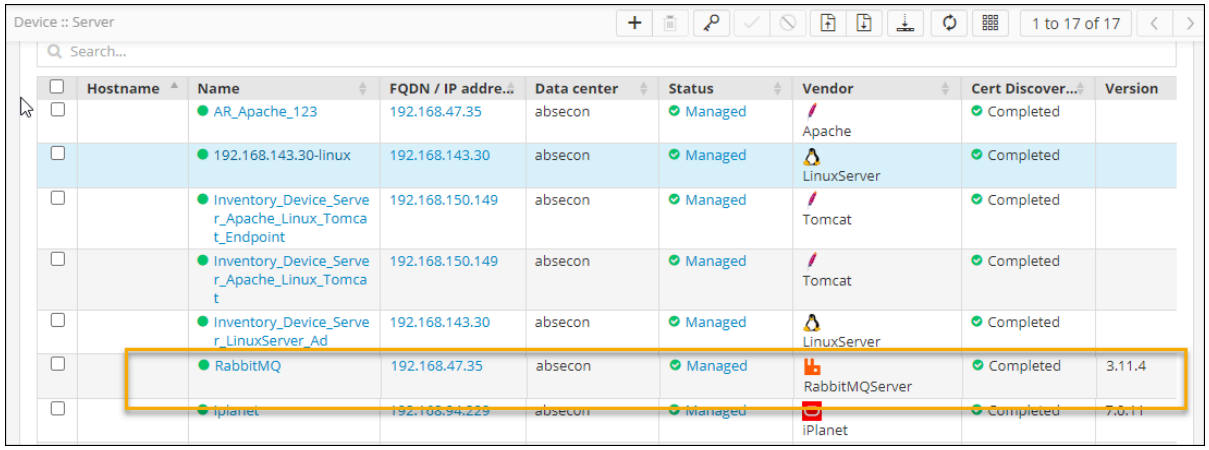
7. In the **Vendor Specific Details** section enter the details as follows.

Vendor Specific Details - Field Description Table

Fields	Description
Config path	Enter the path where the config file is saved. *Example:*etc/rabbitmq/rabbitmq.config
**: Mandatory fields*	

8. Click **Save**.

   The device is on-boarded successfully and the version number in the **Version** column will contain the value **3.11.4**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

SAP

Prerequisites

WebDispatcher

- Ensure the target server IP is accessible from the cloud connector and the port is open.
  1. To SSH into a machine using a specific port, use:

     ```
     ssh -p <port_number> <username>@<hostname_or_ip_address>
     ```

- If **access elevation is set to *None***, the application or service users must have the necessary read/write permissions to perform CLM actions on the target server. Commands in this case are executed using the following format:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- `su - {sid}adm -c "some_command"`
  - If the SAP SID is configured with password authentication, the command will prompt for it. In such cases, ensure the password is provided in the user interface.
- When **access elevation is set to *sudo* or *dzdo***, the application runs commands using the following format:
  - `sudo su - sidadm -c "some_command"`
  - This means the current SSH user needs permission to run `su - {SAPSID}adm` via `sudo`.
  - Make sure the ssh user is added to the sudoers file to execute the sudo/dzdo command.
  - AppViewX supports both password-enabled and passwordless sudo execution.
- The installation path is based on the user ID. The user ID will be <SAPSID>adm.
- We use **SFTP** for file transfers (certificate push), so it's crucial to ensure that SFTP is properly configured for the logged-in user
  1. From the cloud connector: You can use the `sftp` command to test the connection to an SFTP server. Open your terminal and type:

     ```
     sftp username@hostname
     ```

  2. Use the `put` command to upload the file to the remote server:

     ```
     put localfile /path/to/remote/directory
     ```

ABAP

Create a Web Service for the Function Module

- SOAMANAGER has to be enabled to create a custom function module in the ABAP to bind the certificate. Authentication details have to be provided on the device onboarding page.
- Use **Basic Authentication** with an SAP technical user (e.g., SAP_RFC) and **HTTPS** for transport security.
- `<protocol>://<deviceIp>:<Web Service Port>/sap/bc/srt/rfc/sap/zws_update_ssl/{Client ID}/zws_update_ssl/zbind_update_ssl`

Onboarding SAP

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select the **SAP** logo from the Vendors list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **SAP** server configuration screen is displayed.

5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type from radio button options. • ABAP • WebDispatcher
***Server name**	Enter the name of the designated SAP server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the SAP.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the SAP server.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • Manual entry (default) • All supported Internal and external vault • SSH

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the username, upload the key file, and enter the passphrase (if the private key is password-protected) for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select *sudo or dzdo* to execute with root privileges using sudo access. The default value is *None.* AppViewX supports both password-enabled and password-less sudo/dzdo execution. **Note:** SSH key-based authentication does not support password-enabled sudo/dzdo.
***Client ID**	**Note:** All these fields are enabled when the **Server Type = ABAP**.
***Web Service User ID**	
***Web Service Password**	
***Web Service Port**	Enter the following details: • Client ID • Web Service User ID

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• Web Service Password • Web Service Port The following fields are required to invoke the web service to bind the certificate into the selected profile. The values entered in the fields are used to frame and invoke the API with the credential. **Note:** For push and bind operations, details of all these fields must be provided.
Is Https?	Select the checkbox to frame the API with http or https.
File Upload Temp Path	Enter the valid file upload directory. The default value is `/tmp/`. **Note:** Both the SSH user and SAP user should have read, write, and execute permission.
**: Mandatory fields*	

8. In the **SAP SID Details** section, enter details as mentioned below.

SAP SID Details - Field Description Table

Fields	Description
***SAP SID Details**	Enter the three digit character code SAP System Identification (SAP SID). It corresponds to the identifier for an SAP system. Enter the values in upper case only.
Password	Enter the valid password. This is required when None access elevation is selected and switching to SAP SID is a password-enabled configuration.
**: Mandatory fields*	

9. Click **Save**.
   The SAP device is added successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pre-Config Fetch

Device communication check

Command	Description	Are the commands executed with `sudo` or `dzdo` when access elevation is enabled in the UI?
`bind 'set enable-bracketed-paste off'`	To disable bracketed paste mode for the current session	No
`su - {sid}adm -c "echo sap"`	The command is used to check the communication	Yes

Config Fetch

Perform **status and configuration checks** for a SAP Web Dispatcher instance.

Command	Description	Are the commands executed with `sudo` or `dzdo` when access elevation is enabled in the UI?
`su - {sid}adm -c "ps -ef | grep {sid}adm | grep sapstartsrv | grep -v grep"`	Check if the SAP Web Dispatcher service (sapstartsrv) is running under the {sid}adm user and collect the SAP instances	Yes
`su - {sid}adm -c "test -d /usr/sap/{SID}/{instance} && echo exist || echo not exist"`	This command verifies the existence of a specific SAP Web Dispatcher instance directory using the `{sid}adm` user. It is executed for each result obtained from the previous command.	Yes
`su - {sid}adm -c "sapcontrol -nr {instanceNr} -function GetVersionInfo | grep sapstartsrv | grep -v grep | cut -d, -f2,3"`	Command retrieves the **version information of the** `sapstartsrv` **process** for the SAP Web Dispatcher instance, using the `{sid}adm` user.	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	Note: Here, instanceNr refers to the last two numeric characters in the Instance ID. If the instance ID is D00, then the -nr should be '-nr 00'.	

Discovery

- SAP uses its cryptographic tool called *sapgenpse*. Using this tool, we can create a .PSE file and export the certificate from the PSE file. (Personal Security Environment).
- **Types of PSE file supported:**
  1. Server Standard PSE (SAPSSLS.pse)
  2. Client PSE
     a. Anonymous (SAPSSLA.pse)
     b. Standard (SAPSSLC.pse)
  3. Web Service PSE (SAPWSSE.pse)

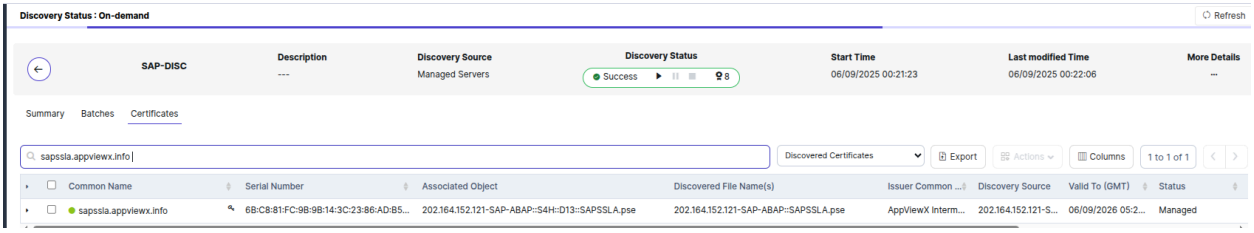
Command	**Description**	Are the commands executed with `sudo` or `dzdo` when access elevation is enabled in the UI?
`su - {sid}adm -c "cd /usr/sap/{SID}/{Instance}; find /usr/sap/{SID}/{Instance} -name SAPSSLS.pse -o -name SAPSSLA.pse -o -name SAPSSLC.pse -o -name SAPWSSE.pse"`	This command checks for the presence of **specific SAP PSE (Personal Security Environment) certificate files** within a given SAP Web Dispatcher instance directory, using the `{sid}adm` user.	Yes
`su - {sid}adm -c "mkdir -p / fileUploadTempPath/{transactionalFolder} "`	This command creates a transactional temp directory inside the `/{fileUploadTempPath}` given in the UI.	Yes
`su - {sid}adm -c "chmod 777 / {fileUploadTempPath}/{transactionalFolder}"`	This command changes the **permissions** of the transactionalFolder to be **rwx by all users** (`777`)	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

su - {sid}adm -c "sapgenpse export_p12 -z \"\" -p /usr/sap/{SID}/{Instance}/sec/{pse} / {fileUploadTempPath}/{transactionalFolder}/SAPSSLA.p12"	This command **exports the SAP PSE (Personal Security Environment) certificate** in **PKCS#12 (.p12) format to the temp directory**.	Yes
su - {sid}adm -c "openssl pkcs12 -in / fileUploadTempPath/{transactionalFolder}/SAPSSLA.p12 -out / fileUploadTempPath/{transactionalFolder}/SAPSSLA.txt -nodes -passin pass:"	To convert the `.p12` certificate bundle into a **plaintext PEM format** containing the certificate and private key,	Yes
su - {sid}adm -c "cat / fileUploadTempPath/{transactionalFolder}/SAPSSLA.txt"	To **view the contents** of the extracted SAP SSL certificate and key file	Yes

Discovery cert-profile association:

For each instance and its supported PSE files, AppViewX will discover the certificates and generate a profile named in the following format:



Profile Naming Convention: deviceName::sid::instance::pse

202.164.152.121-SAP-ABAP::S4H::ASCS14::SAPSSLC.pse
202.164.152.121-SAP-ABAP::S4H::ASCS14::SAPSSLS.pse

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CSR Generation at Endpoint

The **Replace PSE File** checkbox enables users to generate the new CSR and private key in the Server. This checkbox is displayed only in the case described below:

1. Select the **CSR Generation** option as **Endpoint**.
2. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names.
3. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated.

The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.

Command	**Description**	Are the commands executed with `sudo` or `dzdo` when access elevation is enabled in the UI?
`su - {sid}adm -c "test -f <file_path> && echo exist || echo not exist"`	Check if the PSE file **exists**and is a regular file.	Yes
`su - {sid}adm -c "cp /usr/sap/S4H/D13/sec/SAPSSLA.pse / usr/sap/S4H/D13/sec/backup/SAPSSLA.pse_bkp_1721623695188"`	This creates a backup of the existing PSE file	Yes
`su - {sid}adm -c "chmod 755 / usr/sap/S4H/D13/sec/backup/SAPSSLA.pse_bkp_1721623695188"`	This command changes the permissions of the backup file.	Yes
`su - {sid}adm -c "rm /usr/sap/S4H/D13/sec/SAPSSLA.pse"`	When Replace PSE Enabled → Then remove the original pse file	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

su - {sid}adm -c "sapgenpse gen_pse -p /usr/sap/S4H/D13/sec/SAPSSLA.pse -r /tmp/S4HD13SAPSSLA-csr-1721623774652.p10 -x \"\" -a RSA:2048:SHA256 -k GN-dNSName:appviewx123.test.com 'CN=appviewx123.test.com'"	When Replace PSE Enabled → Generates a new SAP SSL PSE file.	**Yes**
su - {sid}adm -c "sapgenpse gen_pse -p /usr/sap/WDP/W00/sec/SAPSSLS.pse -onlyreq -r /tmp/incorrectprofile.p10 -x "" -a RSA:2048:SHA256 -k GN-dNSName:incorrectprofile "CN=incorrectprofile""	When Replace PSE Not Enabled → this command would create the Certificate Signing Request (CSR), not the full PSE file	**Yes**
su - {sid}adm -c "cat /tmp/S4HD13SAPSSLA-csr-1721623774652.p10"	Read the CSR content	**Yes**
su - s4hadm -c "rm -f /tmp/S4HD13SAPSSLA-csr-1721623774652.p10"	Remove this transactional file created to hold the CSR content.	**Yes**

Push Support

- Only the certificate enrolled at the endpoint can be pushed to the end device.
- [WebDispatcher] The certificate in P12 format will be uploaded to the SAP temporary directory using SFTP.
- Pushing Root and Intermediate Certificates is enabled by default and cannot be disabled.
- [WebDispatcher] Based on the profile selection, select the **PSE Type**.
- Select the same profile that is used to enroll a certificate at the endpoint.

Bind Support

WebDispatcher

Command	**Description**	Are the commands executed with `sudo` or `dzdo` when access elevation is enabled in the UI?

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

su - {sid}adm -c "sapgenpse import_own_cert -p /usr/sap/WDP/W00/sec/SAPSSLS.pse -c /tmp/SAPSSLS_W00_temp_20250530084259.txt"	Import the pushed certificate from the temp directory to the selected profile PSE file.	Yes
su - <SID>adm -c "sapgenpse get_my_name -p /usr/sap/WDP/W00/sec/SAPSSLS.pse	Check if the bind is successful.	
su - {sid}adm -c "rm -f /tmp/SAPSSLS_W00_temp_20250530084259.txt	Remove the temp transactional file	Yes
The below commands will be executed based on the Service restart request		
su - <SID>adm -c "sapcontrol -nr <instance_number> -function Stop"	Stops the SAP instance	Yes
su - <SID>adm -c "sapcontrol -nr <instance_number> -function GetProcessList"	To check if the instance is stopped fully.	Yes
su - <SID>adm -c "cleanipc <instance_number> remove"	This command cleans up IPC resources like shared memory and semaphores that may not have been properly released, usually after an unclean SAP shutdown.	Yes
su - <SID>adm -c "sapcontrol -nr <instance_number> -function Start"	To start the SAP instance	Yes

ABAP

```
curl -kv -X POST "https://{ip}}:44313/sap/bc/srt/rfc/sap/zws_update_ssl/300/zws_update_ssl/zbind_update_ssl" \
 -H "Content-Type: text/xml;charset=UTF-8" \
 -H "SOAPAction: urn:sap-com:document:sap:soap:functions:mc-style:ZUpdSslCert" \
 -u <Web Service User ID>:<Web Service Password> \
 --data '<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:urn="urn:sap-com:document:sap:soap:functions:mc-style">
 <soapenv:Header/>
 <soapenv:Body>
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  <urn:ZUpdSslCert>
    <ImOwncert>X</ImOwncert>
    <ImCert>
      ...root, Intermediate and signed certificate.
    </ImCert>
    <ImPsename>{PSE_FILE_NAME.pse}</ImPsename>
    <ImHost>{HOSTNAME}</ImHost>
    <ImInstanceno>{INSTANCE_ID}</ImInstanceno>
  </urn:ZUpdSslCert>
 </soapenv:Body>
</soapenv:Envelope>'
```

The response XML will be as follows:

```
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
  <soap-env:Header/>
  <soap-env:Body>
  <n0:ZUpdSslCertResponse xmlns:n0="urn:sap-com:document:sap:soap:functions:mc-style">
    <ExError/>
  </n0:ZUpdSslCertResponse>
  </soap-env:Body>
</soap-env:Envelope>
```

If the ExError tag is empty, it means the certificate updation is successful. If there are any errors, the ExError tag will have ‘X’ in it and another tag ExText will contain the error details.

Note: In the event of a failure during the bind operation, an automatic rollback will be performed by restoring the backup PSE file.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.

4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Limitations

WebDispatcher

SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. So if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.

ABAP

Service Restart functionality has been disabled for SAP ABAP. Use the postscript execution.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Tomcat (Linux)

Refer to Automating CLM for Tomcat (Linux).

Tomcat (Windows)

Prerequisites

- The Tomcat server must be in the running state. This can be validated by checking services in Windows Task Manager.
- Ensure that the target Hostname is accessible from the Windows Gateway Agent.
- The user must have the necessary permissions to access, download, and upload the **server.xml** and the certificate files associated with the configured settings. (Read and Download permissions should be granted to the user as configured.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The directory path containing the **server.xml** file must be specified as the **Installation Directory** during device onboarding.
- Users can manage the Tomcat installed on any drive; however, the account used to manage Tomcat in AppViewX must be configured as a **local administrator** and must have access to both the **Installation Directory** and the **server**.
- Tomcat must be present in the specified directory path, where at least one folder name should include Tomcat.
- To perform certificate discovery, SSL must be enabled on the connector for the respective service. `SSLEnabled="true"` ensures that the connector supports SSL, which is required for certificate discovery.
- Certificates located in paths without the required user permissions cannot be identified. Ensure that the certificates are either configured in the configuration files using accessible paths or update the file permissions to allow the user to access them.
- The system supports **Tomcat**, **ADManager**, and **AD Self Service Plus**. Profiles are automatically created based on the respective installation paths. During the push operation, use the **Device Selection** dropdown to choose the service and view the profiles created for it.

Onboarding Tomcat (Windows) Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Microsoft** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server Details - Field Description Table

Field	Description
***Server Type**	Select the **Tomcat** radio button.
***Server name**	Enter the name of the designated Apache Tomcat server.
***Hostname**	Enter the hostname of the Apache Server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Apache server. Gateway is the preferred communication mode.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache (Tomcat) server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Field	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Field	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount (when the communication mode is SSM) • All supported external vaults **Note:** • Credential Type does not suppot ssh based authentication for Microsoft devices. • If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Example: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. Enter the **Windows gateway details**.

> **Note:** This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Field	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode **Note:** The integrated gateway functionality is not compatible with the following features: • Server addition using the **import** feature • Endpoint CSR generation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI. **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • **Remote** **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. From the following options, select the gateway: • New • Existing
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Field	Description
Server path	Enter the directory/path where the application is installed. Tomcat ADManager & Self Service Plus has to be integrated under Windows Tomcat, so the paths can be defined as follows: • C:\<parent_folder> e.g. C:\ProgramFiles - Certificates will be discovered from Tomcat, ADManager & Self Service. • C:\ProgramFiles\Apache-Tomcat-8.5.35 - Certificates will be discovered only from Tomcat. • C:\ProgramFiles\ManageEngine\ADManager - here the certificates will be discovered only from ADManager. • C:\ProgramFiles\ManageEngine\ADSelfService - here the certificates will be discovered only from ADSelfService
**: Mandatory fields*	

9. Click **Add.**

   Once the server is added successfully, the path will be listed in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. *[Optional]* Click the (**Delete**) icon, if you want to delete the server path from the list.
11. Click **Save**.
    The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the **Status** column, click Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

VMware

Prerequisites for vCenter

1. Make sure the vCenter device is reachable from the cloud connector.
2. Support is only for **vCenter 7.0.3 or later** (REST API-based).
3. Minimum permissions required to run the CLM operation in AppViewX for the vCenter User is:
   - Role > Certificate Management > Create/Delete (Admins priv)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding VMware

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **VMware** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select server type as **VMWare NSX** or **VMWare vCenter** from the dropdown list.
***Server name**	Enter the name of the designated VMware server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the VMware.
Data center	Select the datacenter for routing communications to this vendor.
HTTPS Port	Enter the port number used for HTTPS communication with the server. By default, it is 443.
Proxy required	Select the checkbox to enable the secure proxy service.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as follows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - AppViewX* **Note:** If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (This field displayed only for manual entry.)
***Password**	Enter the secure password. (This field displayed only for manual entry.)
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, enter details as mentioned below.

Note: This section is displayed only for **VMWare NSX** device.

Vendor Specific Details - Field Description Table

Fields	Description
***Base URL**	Enter the base URL that is to be appended with the API. *Example*: /policy/api/v1
**: Mandatory fields*	

8. Click **Save**.
   The VMware device is added successfully.
9. On onboarding VMWare vCenter, run two REST APIs: `GET Session` (to fetch the session ID to authorize and to confirm communication with the vCenter device) and `GET Version` (to fetch the vCenter version).

Note: REST API is used for vCenter version 7.0.3 and later.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The VMWare vCenter device can also be onboarded by the import functionality using the standard .xlsx and .csv templates available.

To onboard the VMWare vCenter device to the AppViewX inventory using the import functionality:

1. Go to **(Menu) > CERT+ > ADMINISTRATION > Device Management.**
2. Click the **Server** tab.
3. Click the (**Import**) icon on top of the page. The Import details page is displayed.
4. Click the CSV or XLSX icons in the **Uploader Info** section.

   The sample templates are downloaded and saved at the default file location.
5. Open the CSV or XLSX templates, enter the relevant information for onboarding the VMWare vCenter device, and save the file.

   Note: Ensure all the mandatory and relevant fields are entered in the .csv or .xlsx template.
6. Click the **Upload** icon in the Import section, and select the .csv or .xlsx file from the file dialog box.

   The status of the uploaded file is displayed in the File Histories section.

Discovering Certificates

Note: This section is application only for VMWare vCenter.

- Discovery (on-demand and scheduled) of certificates via REST API includes:
  - Machine SSL
  - STS Signing (`active_cert_chain`)
  - Trusted Root certificates
- The system creates the following certificate profiles with the correct naming convention:

Certificate Profile	Naming Convention
Machine SSL	`{deviceName}:machineSSL`
STS Signing (`active_cert_chain`)	`{deviceName}:stsSigning`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Profile	Naming Convention
Trusted Root certificates	{deviceName}:trustedRoot

Note:

- To enable push operations from the root and intermediate inventory, a trustedRoot profile has been created. To add a connector for VMWare NSX, select VMWare from Vendor.
- **Limitation:** As the private key is never exposed via API, discovered certificates do not include the private key.

Pushing Certificates to the Device

- Admin can select Machine SSL or STS Signing as the target certificate type.
- The system validates the certificate chain in the following order: Server Certificate → Intermediate CA → Root CA
- Users can select both Machine SSL and STS Signing profiles for a single push operation.
- **Machine SSL supported scenarios:**
  - CSR was previously generated and the private key is securely stored.
  - The root CA of the signed certificate is:
    - Already trusted by vCenter → No additional trust configuration required.
    - Not trusted by vCenter → The root CA certificate must be added during the operation.
- **STS Signing supported scenarios:**
  - The certificate must include the private key and the trust (root/intermediate) certificate(s).
  - If either the private key or trust certificates are missing, the operation will fail in the backend.
- **Trust Store Handling**
  - If the root CA is already trusted, the system installs only the certificate and the private key (if required).
  - If the root CA is not trusted, the system installs the certificate, the private key, and the root CA certificate, and updates the trust store.
  - The operation will succeed only if the trust chain is complete and valid.
- **Logging & Audit**

  All certificate push attempts are logged with user, timestamp, certificate type, and result.

- **Error Handling**

  The system displays user-friendly error messages for invalid input, trust chain failures, or installation errors.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

1. If VMware Appliance Management Interface does not display the new certificate after replacing the MACHINE_SSL_CERT on vCenter Server Appliance, refer to https://knowledge.broadcom.com/external/article?legacyId=2136693
2. For stopping, starting, or restarting VMware vCenter Server Appliance services, refer to https://knowledge.broadcom.com/external/article/344633/stopping-starting-or-restarting-vmware-v.html

Backing Up and Rolling Back Certificates

- **Backup**: The existing vCenter certificate is backed up before replacement.
- **Private Key Limitation**:

  The private key cannot be backed up. Rollback is possibleonly if the private key is already stored in AppViewX for the corresponding backup certificate UUID.

- **Rollback Support**:
  - Rollback option is available only if the push is successful and the backup certificate's private key is present in AppViewX.
  - Not applicable for certificates enrolled directly at the endpoint.

  Once a certificate is pushed for an enrolled private key, further pushes are not allowed for that key.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The **Server Inventory** page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Device Status Log pop-up is displayed.

5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Gigamon

Prerequisite

- Enable API access on GigaVUE-FM to facilitate integration.
- Configure role-based access control (RBAC) to allow users to manage certificates securely.
- Ensure proper network connectivity between GigaVUE-FM and AppViewX/CC for seamless communication.
- Verify that all necessary communication ports are open and accessible.
- For Inbound and Outbound Inline-SSL deployments, configure the keychain password before installing certificates and private keys into the keystore.

Onboarding Gigamon

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select the **Gigamon** logo from the Vendors list.
5. In the **Server details** section, select/enter the details as follows

Server Details - Field Description Table

Fields	Description
***Server Type**	The value is set to GigaVueFM.
***Server name**	Enter the name of the designated Gigamon server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***IP address/FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the GigaVue Appliance that is to be onboarded.
HTTPS Port	Enter the HTTPS port number used for secure communication.
Data center	Choose the desired data center.
Proxy Required	Enable this field if GigaVue communication needs to occur via a Proxy. The proxy details configured in general settings will be used for communication.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback, and so on.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *All other external Vault*.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • All other vault settings (BeyondTrust, Cyberark, Hashicorp Vault, Thycotic, and so on.) configured in the **Credentials** will be displayed in the dropdown.
***Username**	Enter the designated username for authentication. **Note:** Field displayed for manual entry only
***Password**	Enter the secure password. **Note:** Field displayed for manual entry only
**: Mandatory fields*	

7. Click **Save**.

Note: Multiple devices can be configured for the same vendor.

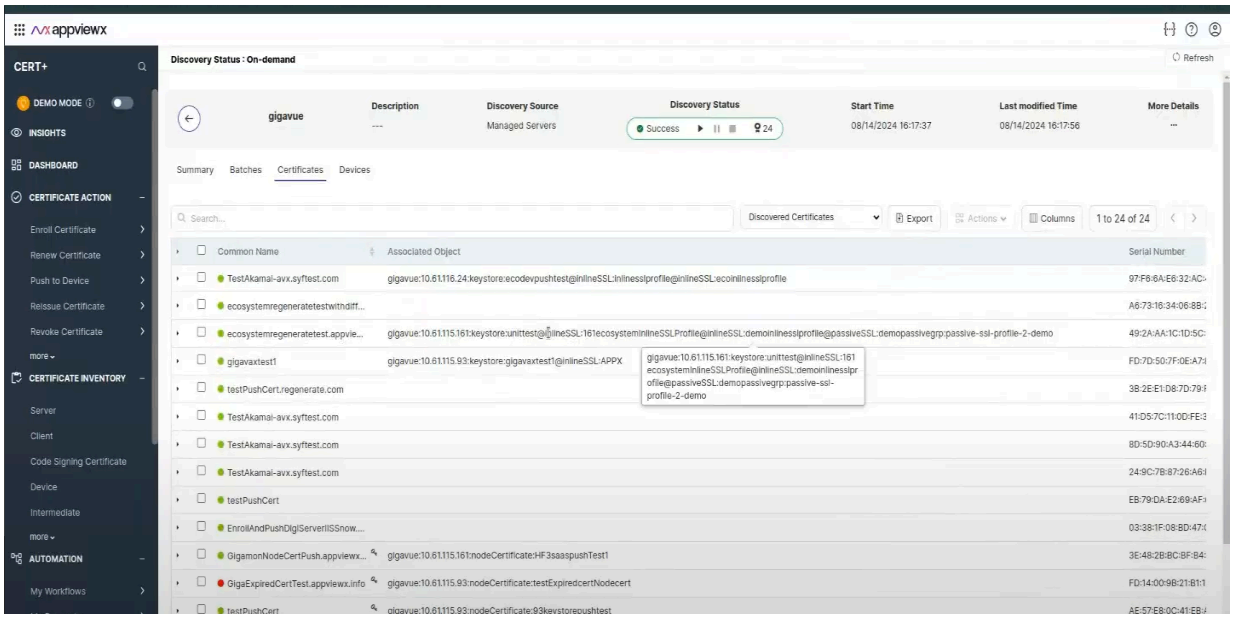
The device is onboarded successfully.

Discovery

- AppViewX automatically detects all clusters and nodes within the Gigamon appliance, enabling comprehensive discovery, push, and bind operations across all nodes.
- For each identified node, AppViewX discovers both the node certificate and any certificates in the keystore, offering detailed visibility into their associations with inline and passive profiles.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Discovery cannot retrieve the private key from GigaVUE-FM.

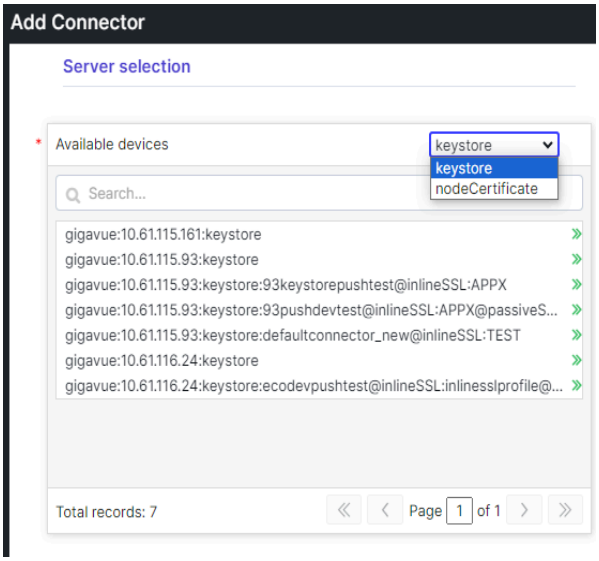


Profile Naming Convention

- Naming convention for profile

Profile	Format
Default Connector: This profile is used for all cluster nodes and is designed to push the certificate to the specified cluster's keystore.	deviceName:clusterId:keystore
Passive: Used to push the certificate to the keystore and bind it to a specific Passive SSL profile.	deviceName:clusterId:passiveSSL:groupName:sslProfileName:certA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Profile	Format
Inline: Used to push the certificate to the keystore and bind it to a specific Inline SSL profile.	deviceName:clusterId:inlineSSL:sslProfileName:certAliasName 

Push Support

- AppViewX enables certificate deployment to the following two destinations:
  - Node Certificate
  - Keystore.
- CERT Type: <.pem> format is supported
- Bit length: Upto 4096
- HASH Type: SHA516
- The Overwrite option is enabled on the App Connector screen to manage push operations for the profile connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- By default, the overwrite option is dissabled.
- If **Overwrite** is enabled, the existing certificate will be deleted and replaced with the new one during the push operation.
- After renewal or regeneration, it is recommended to use a different alias name. This approach avoids deleting the old certificate; instead, its association is removed, and the newly pushed certificate is assigned to the profile.

Note:
- The keystore certificate is shared by both inline SSL and passive SSL.
- During the push operation, the certificate is pushed into the keystore.
- Within a cluster, the alias name or certificate name must be unique.
- The same certificate cannot be imported to a GigaVUE-FM node using a different alias name.
- Certificate and alias names are unique within a cluster.
- The same certificate with the same name can be pushed to a different cluster.
- To push a certificate into GigaVUE, the private key is mandatory.
- The same certificate can be mapped to multiple profiles.

Bind Support

- AppViewX allows the binding of certificates to the following profile types:
  - Inline Profile
  - Passive Profile.

Note:
- Depending on the selected profile (default or device profile), the certificate is bound to that profile.
- Both inline and passive profiles share the same keystore. For example, a certificate pushed to the keystore becomes available to both passive and inline SSL profiles.
- AppViewX supports SSL operations only for existing profiles in the Gigamon environment.
- Profile creation must be performed outside of AppViewX.
- During device onboarding, AppViewX automatically discovers all available nodes in the Gigamon environment.
- Backup functionality is not supported; as a result, rollback operations cannot be performed.
- Private key export is not supported due to security restrictions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Limitations

The following limitations apply:

- **Private Key Retrieval**: Discovery cannot fetch the private key from Gigavue-FM.
- **Certificate Deployment**: Pushing a certificate to Gigavue requires the private key to be available.
- **Discovered Certificates**: Discovered certificates cannot be pushed to Gigavue unless they are regenerated or renewed within AppViewX.
- **Backup and Rollback**: These features are not supported, as the system cannot back up the private key.
- **Endpoint Enrollment**: Enrollment at the endpoint is not supported because Gigamon has confirmed that the API is not fully functional.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

PingFederate

Onboarding PingFederate

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select **Ping Identity** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select Server type has default value **PingFederate**.
***Server name**	Enter the name of the designated PingFederate server.
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) of the device being onboarded. It is used for device communication and integration with the server.
***HTTPS Port**	Enter the valid HTTPs port number that is required to remotely access iDRAC through firewall.
Data center	Select the datacenter from where communication needs to be routed to the PingFederate instance.
Proxy Required	Select the checkbox if proxy is required.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication with the PingFederate server.
***Password**	Enter the secure password.
*: Mandatory fields	

7. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
***Base URL**	Enter the base URL to communicate with PingFederate API. For example, **/pf-admin-api/v1/**.
*: Mandatory fields	

8. Click **Save**.
   The PingFederate device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What's Next

Once you have onboarded and validated the device connection, you are ready to proceed with the any of the following certificate actions:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.
- If you want to enroll a new server certificate, see Enrolling a Server Certificate.

Deleting a Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the checkbox beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the **Delete** icon in the command bar.
   The **Delete** confirmation pop-up window is displayed.
5. Click **Yes** on the confirmation pop-up.
   The server will be removed from the inventory

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Importing a Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the checkbox beside the device name.

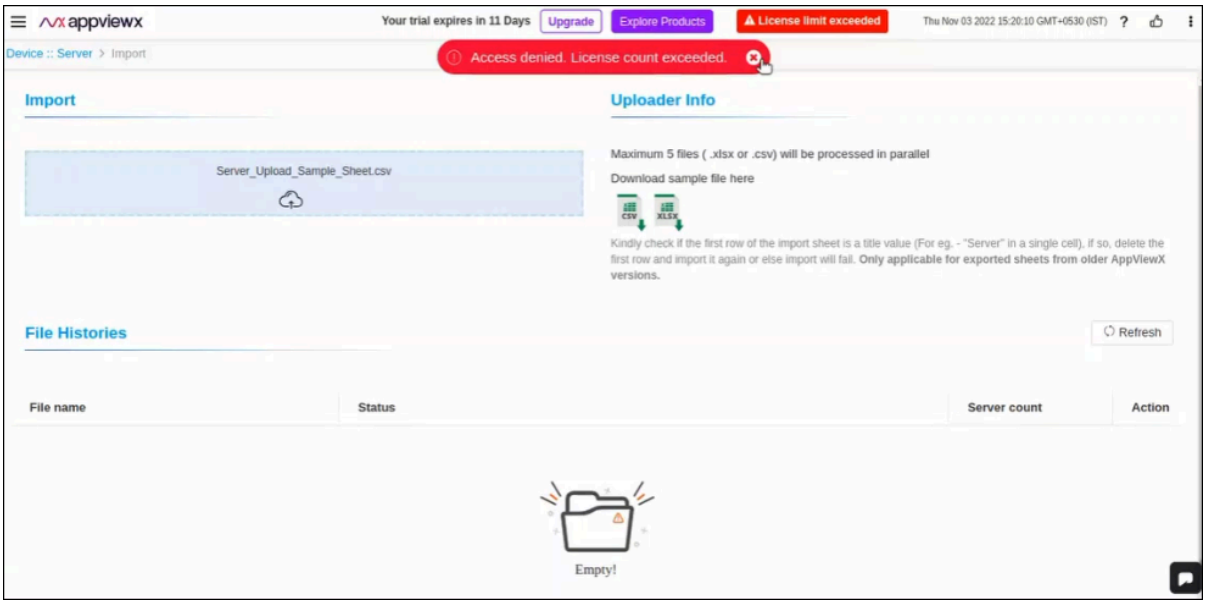
> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Import**) icon in the command bar.
   You will be redirected to the import server page.
5. Download the sample <.csv> or <.xlsx> file.
   a. The **XLSX** option enables you to download a vendor-specific file with ease:
      i. Click the **XLSX** file icon.
      ii. From the **Vendors** field, select the desired **vendor** from the dropdown list.
      iii. Click **Download** to get the file.
6. Update the details.
7. Click the **Browse** and **Upload** button.
8. Upload the files.
   Sever details provided in the sheet will be added to the server inventory.

License Enforcement

AppViewX has enabled a feature to set a limit for the licensed certificates. If the number of certs exceeds this limit then the additional certs added into the inventory will be moved into the **Monitored** status.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- A red indicator labelled **License Limit Exceed** is displayed on the title bar of the page, if the limit has exceeded.
- A pop-up message **Access denied. License count exceeded** is displayed on the click of the **Save** button while adding a new server device.

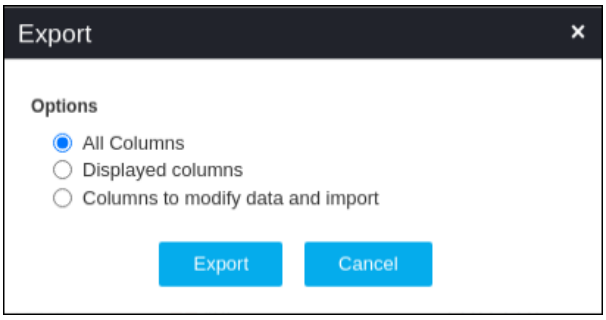
Exporting a Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the check-box beside the device name. If you are exporting details of multiple servers of the same kind, select the check-boxes for each one.

   Note: If the desired server device is not listed on the screen, run a search.

4. Click the (**Export**) icon in the command bar at the upper right of the screen.
5. On the Export pop-up, select the type of information you want to export and click the **Export** button.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



a. **All Columns** - Select this option if you want to export all information about the server.
b. **Displayed columns** - Select this option if you want to export only the information that is visible on the server screen. This is useful if you need to compare values or settings for different servers and do not have any need to see the less important data.
c. **Columns to modify data and import** - Select this option if you are exporting device details to make modifications and then re-import the data into the Device Inventory.

6. On the screen that opens, select the location where you want the device details file to go, then click **Save**.
   Server details will be downloaded as an Excel `<.xls>` file.

Managing a Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the checkbox beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. To start managing the device, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   • The "Config fetch" will be triggered and the server will get managed.
   • The server status is changed to Manage.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Unmanaging a Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the checkbox beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the Command bar at the top of the screen.
5. Click the **Yes** button from the confirmation popup message that is displayed.
   Server device status is changed to UnManaged in Server inventory.

Executing Fetch Config for Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the checkbox beside the device name.

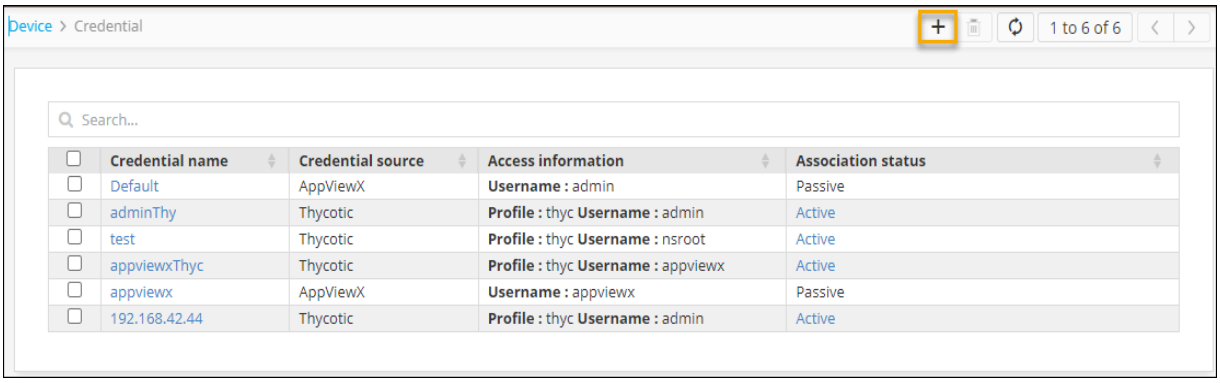
> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the server.** The configuration will be fetched from the server.

Adding Device Credentials

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Credentials**) icon in the command bar.
   The Credentials page is displayed. If credentials have been set up, a list of credential names with details will be displayed in a table as shown below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. To add a new credential, click the plus or + (**Add**) icon in the command bar of the Credentials page.
   The Add Credential page is displayed with default credentials fields for AppViewX.

> **Note:** For details of fields in AppViewX and other vaults refer to the sections below.

AppViewX

AppViewX is shipped with a built-in integration with HashiCorp Vault for software level security to secure the private keys and device credentials onboarded to the product.

To configure credential details for the AppViewX enter the fields described in the table below.

Field Description for AppViewX Credentials

Fields	Description
***Credential name**	Name for the credential for the users to identify it.
***User name**	User name used for device onboarding.
Credential type	Select the type of authentication from one of the following: • Password • Identity key
***Password**	Password configured at the time of device onboarding.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for AppViewX Credentials (continued)

Fields	Description
	Note: This field is displayed only when the **Credential type** is selected as **Password**.
Secondary password	Additional password enabled by vendors for specific operations. **Note:** This field is displayed only when the **Credential type** is selected as **Password**.
***Identity key**	Credentials (private key in the **.pem** or **.txt** format) for enabling device communication via SSH. **Note:** This field is displayed only when the **Credential type** is selected as **Identity key**.
Passphrase	Key to protect the private key files. **Note:** This field is displayed only when the **Credential type** is selected as **Identity key**.
All * marked fields are mandatory.	

Cyberark

To configure credential details for the CyberArk vault enter the fields described in the table below.

Field Description for Cyberark Credentials

Fields	Description
***Credential name**	Name for the credential for the users to identify it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Cyberark Credentials (continued)

Fields	Description
Type	To retrieve a credential from the CyberArk vault, select one of the following options: • Device (default) • Amazon (AWS/ELB)
***User name**	User name that has been added in CyberArk. **Note:** This field is displayed when the **Device** type is selected.
***App ID**	App ID that has been authorized to provide access to CyberArk and retrieve credentials. **Note:** This field is displayed when the **Device** type is selected.
User type	From the dropdown list menu, select one of the following: • Internal (user created directly in the device) • External (user created in the Active Directory) **Note: *Server IP Address** field is displayed when the **User type** is selected **External**.
***Server IP Address**	Server IP Address has to be entered if the user has created external active directory. **Note:** This field is displayed when the User type is selected as **External**.
***AWS IAM username**	User name that has been added in CyberArk.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Cyberark Credentials (continued)

Fields	Description
	Note: This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***App ID**	Reference ID provided by CyberArk for the corresponding application. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
***AWS access key ID**	Access key ID generated from the AWS management console. **Note:** This field is displayed when the **Amazon** (AWS/ELB) type is selected.
Note: The asterisk (*) symbol indicates a mandatory field.	

To configure credential details for the CyberArk vault, from the top right corner of the page, click **CyberArk API Settings**.

Field Description for Cyberark API Settings

Fields	Description
***IIS-Server IP/Hostname**	Hostname or IP address of the CyberArk application.
***Port**	Port number on which CyberArk is running.
***Client certificate**	Upload the Client Certificate needed to authenticate the CyberArk API service.
***Passkey**	Enter the passkey for Client Certificates uploaded in the .pfx format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Cyberark API Settings (continued)

Fields	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

HashiCorp

To add credentials for HashiCorp Vault enter the fields described in the table below.

Field Description for HashiCorp Credentials

Fields	Description
***Credential name**	Unique name for the credential for the users to identify it.
***API Profile**	Select the API profile from the dropdown list which is configured in HashiCorp API settings.
***Secret Engine**	Type path and click enter. It will suggest a list of secrets and the desired secret can be selected.
Note: The asterisk (*) symbol indicates a mandatory field.	

To set API Credentials: From the top right corner of the page, click **HashiCorp API Settings**.

Field Description for HashiCorp API Settings

Field	Description
***API Profile Name**	Enter a unique API profile name.
***IP/Hostname**	Enter the HashiCorp vault hosted IP address or hostname.
***Port**	Enter the port in which the HashiCorp vault is running.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for HashiCorp API Settings (continued)

Field	Description

***Auth Method**	From the dropdown list list, select either **Token/AppRole.**
	
	• If **Token** is selected, enter the **Vault Token** for the authentication.
	• If **AppRole** is selected, enter the following:
	  • Enter the **RoleID**
	  • Enter the **SecretID**

Namespace	Enter a namespace.
Note: The asterisk (*) symbol indicates a mandatory field.	

Thycotic

To add credentials for Thycotic secret enter the fields described in the table below.

Field Description for Thycotic Credentials

Fields	Description
***Credential name**	Reference name for Thycotic in AppViewX.
***API Profile**	If you have more than one Thycotic Server added as profiles, select the respective profile while adding credentials.
Account Type	Select the account type linked with the secret key. The available options are: • **Device** • **Amazon (AWS/ELB)** • **User/Service Account**.
***Credential Type**	Select the type of credential. The available options are: • **Pasword** • **Private Key**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Thycotic Credentials (continued)

Fields	Description
***User Name**	Enter the username of the secret if you selected the account type as **Device** or **User/Service Account**.
AWS IAM Username	Enter the AWS IAM username if you selected the account type as A**mazon (AWS/ELB)**.
Secret Name	Select secret type as Device or Amazon (AWS/ELB) or User/Service Account.

Note: The asterisk (*) symbol indicates a mandatory field.

To set API Credentials: From the top right corner of the page, click **Thycotic API Settings**.

Field Description for Thycotic API Settings

Fields	Description
***API Profile Name**	Reference name for the vault in AppViewX.
***Hostname/Domain Name**	Enter the Hostname of the Thycotic Secret Server if it is hosted in an on-prem environment or the Domain name of the Thycotc Secret Server if it is the cloud version.
***Port**	Port number of the Thycotic Secret Server.
***Type**	Select if Thycotic Secret Server is hosted in an On prem or Cloud environment.
***Username**	Username of Thycotic Secret Server.
***Password**	Password of Thycotic Secret Server.

Note: The asterisk (*) symbol indicates a mandatory field.

Note: You can add multiple Thycotic Secret Servers as different Profiles. Each Thycotic Secret Sever will be added to the Thycotic API settings page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

BeyondTrust

To add credentials for BeyondTrust Vault enter the fields described in the table below.

Field Description for Beyond Trust Credentials

Fields	Description
***Credential name**	Reference name for BeyondTrust in AppViewX.
***API Profile**	If you have more than one BeyondTrust Server added as profiles, select the respective profile while adding credentials.
***Secret Type**	Select the secret type as Device. Only secrets associated with any device can be added with this secret type. i.e., Secret should contain the device name.
Username	Enter the username of the secret if you selected the Secret Type as Device. When this secret is used in any device, respective device name will be automatically send as one of the argument when AppViewX fetches credential from Vault.
Note: The asterisk (*) symbol indicates a mandatory field.	

To set API Credentials: From the top right corner of the page, click **BeyondTrust API Settings**.

Field Description for Beyond Trust API Settings

Fields	Description
***API Profile Name**	Reference name for the vault in AppViewX.
***Hostname/Domain Name**	Enter the Hostname of the BeyondTrust Secret Server if it is hosted in an on-prem environment or the Domain name of the BeyondTrust Secret Server if it is the cloud version.
***Port**	Port number of the BeyondTrust Secret Server.
***Username**	Username of BeyondTrust Secret Server.
Password	Password of BeyondTrust Secret Server.
***API Key**	It is the security key provided for authentication.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Beyond Trust API Settings (continued)

Fields	Description
Note: The asterisk (*) symbol indicates a mandatory field.	

Note: You can add multiple BeyondTrust Secret Servers as different Profiles. Each BeyondTrust Secret Server will be added to the BeyondTrust API settings page.

Enabling Vault as a Service

Vault as a service refers to the provision of Vault, a popular tool for securely storing and accessing sensitive information. It implies that all the vaults and credentials from the platform can be in all the applicable places. For example, if a new credential type feature is supported in the platform, then those credentials will be available to all the vendors in the Server addition page. You do not have to manually make changes for supporting the same in the respective module. The following credentials are now made available to all vendors on the Server device addition page:

- CyberArk
- Thycotic
- HashiCorp
- BeyondTrust

Vault as a service enables the following capabilities:

- Fetches all available credential store from platform.
- Removes the Static Credential type drop down List maintained from Web.
- Consumes the retrieved vaults from platform at required places.
- Vaults are automatically listed in consumption places (e.g. Server device addition)when added in Platform.
- Sets the access list based on user-selected credential type from the available vaults.
- Supports all the vault services of the imported vendors servers.

Configuring Device Setting

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Linux

The **Certificate Details** and **Vendor Specific Details** settings can be configured globally under Device Settings. These configurations will automatically apply to all connectors created and associated with certificates in the inventory. This minimizes redundant configuration tasks when a customer needs to add hundreds of connectors with the same settings.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Device Settings**) icon.
4. Select **Linux** logo from the Vendors list.
   The Linux Vendor Specific Details configuration screen is displayed.
5. In the **Certificate Details** section, select/update the following fields.

Description of fields on the Certificate Details section.

Fields	Description
***Certificate Directory**	Provide the directory where the certificate must be discovered. **Note:** By default, system will scan for certificates from all the directories.
***Operation**	Select the required option from the dropdown list. Available options are, • Include • Exclude.
Scan Type	Select the type of scan. Available options are, • Default • Aggressive.
* (asterisk): *Mandatory fields*	

6. In the **Vendor Specific Details** section, select/update the following fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Description of fields on the Vendor Specific Details section.

Fields	Description
Enable Network Scan	Select the checkbox to enable the network scan.
Certificate Ownership & Permission	Click the radio button to enable the **Certificate Ownership & Permission** option. **Note:** By default, this option is disabled.
Update System TrustStore	Click the radio button to enable the **Update System TrustStore** option for root and intermediate certificates. **Note:** By default, this option is disabled.
* (asterisk): *Mandatory fields*	

7. Click **Update**.
   The vendor details are saved successfully.

AKAMAI CPS

During enrollment using server device as endpoint, Akamai has a long list of details that are mandatorily required for the enrollment request. Adding these fields along with the CSR parameters will make the enrollment form too big with many details to be filled out. Since these are fixed values and only have to be filled once, the other mandatory fields are made available in the global device settings page. The details saved on the global setting page are based on the combination of the fields **Validation Type**, **Secure Network**, and **Vendor Certificate Type** that are available on the enrollment page.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Device Settings**) icon.
4. Select **Akamai** logo from the Vendors list.
   The Akamai Vendor Specific Details configuration screen is displayed.
5. Enter the fields in the respective sections described in the table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Description of fields on the Vendor Specific Details page.

Fields	Description
General Information	
***Validation Type**	Select a validation type from the dropdown list for the endpoint. The default value is **Third-party**.
***Secure Network**	Select the secure network from the dropdown list for the endpoint. The default value is **Standard TLS**.
***Vendor Certificate Type**	Select a vendor certificate type from the dropdown list for the endpoint. The default value is **Third-party**.
Organization Information	
***Name**	Enter the organization's name.
***Address**	Enter the organization's address.
***Country**	Enter the organization's country code.
***City/Municipality**	Enter the organization's city or municipality.
***State/Province**	Enter the organization's state or province.
***Zip/Postal Code**	Enter the organization's zip or postal code.
***Phone Number**	Enter the organization's phone number.
Admin Contact Information	
***First name**	Enter the administrator's first name
***Last name**	Enter the administrator's last name
***Phone number**	Enter the administrator's phone number
***Email**	Enter the administrator's email
Tech Contact Information	
***First name**	Enter the technical contact's first name
***Last name**	Enter the technical contact's last name
***Phone number**	Enter the technical contact's phone number
***Email**	Enter the technical contact's email

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
* (asterisk): *Mandatory fields*	

6. Click **Update**.
   The vendor details are saved successfully.

Microsoft SQL

The **Force Encryption** and **Registry Restart** settings can be configured globally under Device Settings. These configurations will automatically apply to all connectors created and associated with certificates in the inventory. This minimizes redundant configuration tasks when a customer needs to add hundreds of connectors with the same settings.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Device Settings**) icon.
4. Select **Microsoft SQL** logo from the Vendors list.
   The Microsoft SQL Vendor Specific Details configuration screen is displayed.
5. Enable the radio button if required.

Description of fields on the Vendor Specific Details page.

Fields	Description
Service Restart	Enabling this option applies configuration changes that require you to restart the SQL Server service.
Force Encryption	Enabling this option enforces encryption for all SQL server connections.

6. Click **Update**.

APACHE Linux

The **Enable Certificate Details** and **Suppress Heartbeat Alerts During Service Restart** settings can be configured globally under Device Settings. These configurations will automatically apply to all connectors created and associated with certificates in the inventory. This minimizes redundant configuration tasks when a customer needs to add hundreds of connectors with the same settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Device Settings**) icon.
4. Select **APACHE Linux** logo from the Vendors list.
   The APACHE Linux Vendor Specific Details configuration screen is displayed.
5. Enable the radio button if required.

Description of fields on the Vendor Specific Details page.

Fields	Description
Enable Certificate Details	Enabling this option will display the deprecated certificate details section in the Add/Modify device from the Apche Linux.
Suppress Heartbeat Alerts During Service Restart	Enabling this option to disable or prevent false alert triggered during Apache service.

6. Click **Update**.

Configuring and Managing Firewalls

Proper configuration ensures firewalls can handle certificate requests, policy enforcement, and threat protection efficiently. This is critical to maintaining network security, as it ensures certificates are correctly managed and firewalls function seamlessly within the overall security infrastructure.

To set up firewalls to manage certificates securely, this section covers instructions for:

- Adding a Firewall
- Deleting a Firewall
- Importing a Firewall
- Exporting a Firewall
- Managing a Firewall
- Unmanaging a Firewall
- Executing a Fetch Config for Firewall

Adding a Firewall

This section covers instructions for:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Adding CheckPoint Firewall Device
- Adding Cisco Firewall Device
- Adding F5 Firewall Device
- Adding Fortinet Firewall Device
- Adding Juniper Firewall Device
- Adding Palo Alto Firewall Device

Adding CheckPoint Firewall Device

Refer to Automating CLM for CheckPoint.

Adding Cisco Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port numbers 22 (SSH)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Certificates are fetched by issuing a direct command to the device through SSH.

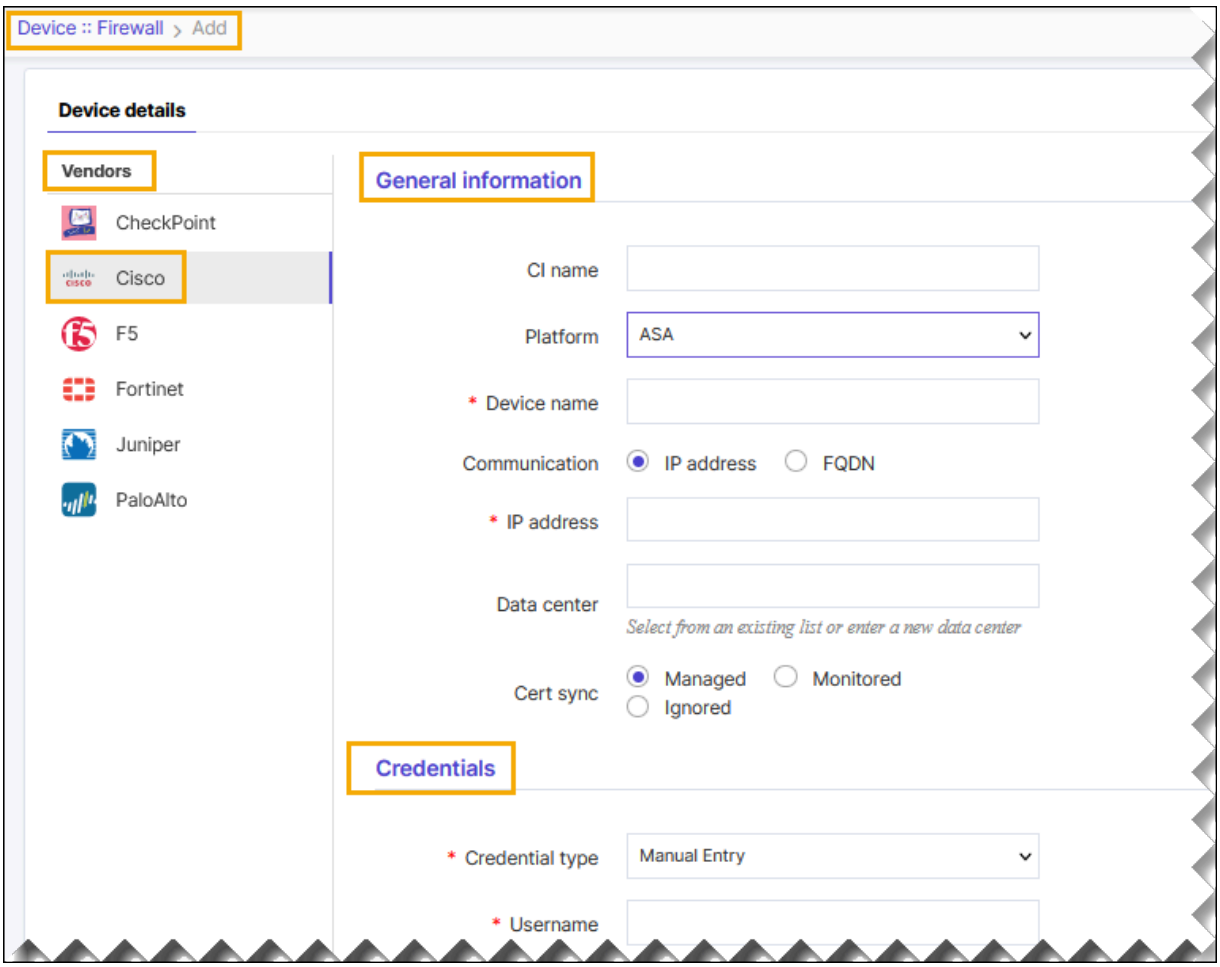
Note: For Visual Workflow action items, you will require credentials with write privilege.

Configuring a Cisco Firewall Device

To add a Cisco device:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Firewall**.
3. On the **Device :: Firewall** page, click (**Add**).
   The **Device :: Firewall > Add** page is displayed.
4. Select the **Cisco** vendor from the left side bar



5. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the dropdown list. The available option is ASA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

6. Enter the field information in the **Credentials** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the dropdown list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the privilege password.
**: Mandatory fields*	

7. Enter the field information in the **Secondary device information** section as follows:
   - **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
   - **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
   - **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

8. Click the **Save** button to add an Firewall device.

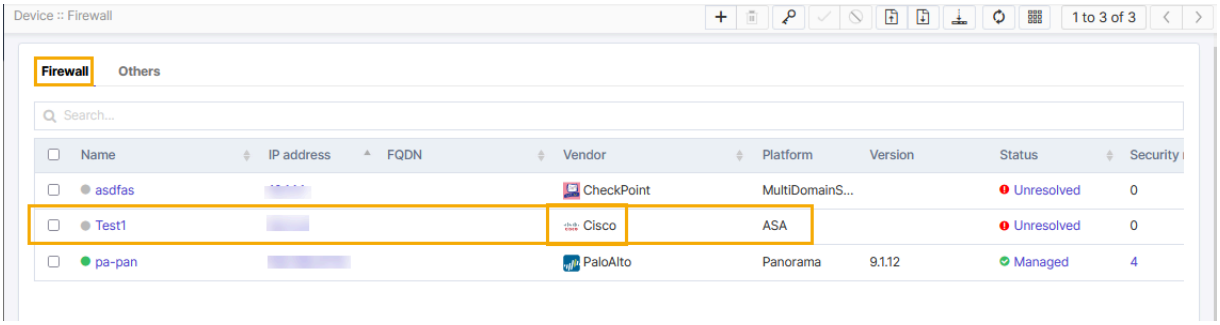
Note:

- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating a Ciso Firewall Device Addition

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Firewall**.
   The **Device :: Firewall** page is displayed. This page is an inventory of all the existing firewall devices.
3. Search the device name and validate whether the device is added successfully.



What's Next

Once you configured the Cisco firewall, you are ready to proceed with the following action to enable the auto enrollment:

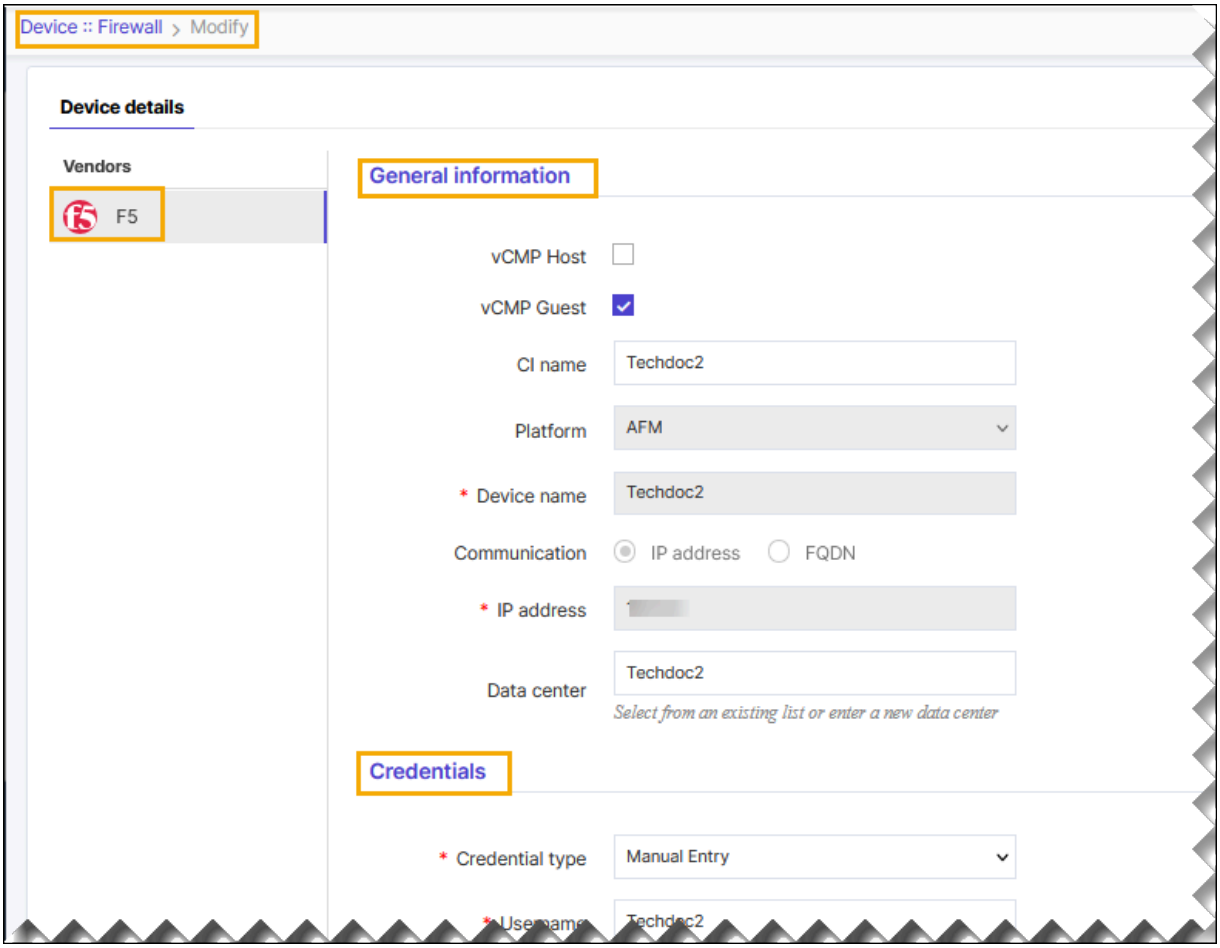
- Automating Certificates for Firewall Devices in AppViewX

Adding F5 Firewall Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring F5 Firewall Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Firewall**.
3. On the **Device :: Firewall** page, click (**Add**).
   The **Device :: Firewall > Add** page is displayed.
4. Select the **F5** vendor from the left side bar.



5. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
vCMP Host	Select the check box to add host based device if required.
vCMP Guest	Select the check box to add device as guest if required..

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the dropdown list. The available option is AFM.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

6. Enter or select the field information in the **Credentials** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the privilege password.
**: Mandatory fields*	

7. **Note:** This step is applicable only if you have selected **vCMP Host** check box in the **General Information** section.

Enter or select the field information in the **Secondary device information** section as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
- **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
- **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

8. Click the **Save** button to add an Firewall device.

Note:

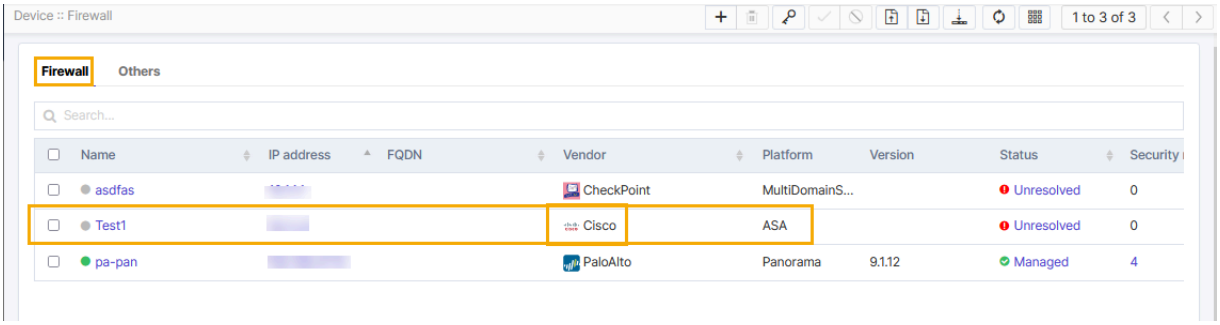
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating F5 Firewall Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Firewall**.
   The **Device :: Firewall** page is displayed. This page is an inventory of all the existing firewall devices.
3. Search the device name and validate whether the device is added successfully.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

Once you configured the F5 firewall, you are ready to proceed with the following action to enable the auto enrollment:

- Automating Certificates for Firewall Devices in AppViewX

Adding Fortinet Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**: Username/Password
- **Services and Port for AppViewX Communication**: Port number 22 (SSH)

> **Note:** For Visual Workflow action items, you will require credentials with write privilege.

Configuring FortiGate Firewall Device

To add a FortiGate device:

1. Go to (**Menu**) > **CERT+** > **Device Management**.
   By default, the **ADC** tab opens.
2. Select the **Firewall** tab.
3. Click the + (**Add**) icon located on the top right corner.
   The **Add** page appears.
4. Select the **Fortinet** vendor from the left side bar.
5. Enter the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select **Fortigate**.
***Device name**	Unique custom identifier of your device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	The data center on which the device has been hosted. Select a datacenter from the dropdown list or enter a data center name.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
***SSH Port**	By default, it is 22.
**: Mandatory fields*	

6. Enter the field information in the **Credentials** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. • If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential Type from the dropdown list. If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your password can be of any length with a combination of alpha-numerical, symbols, and special characters.
Api token	Enter the API token.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

7. Enter the field information in the **Certificate specific details** section.

Field and Description Table

Field	Description
Discover Private Keys	Select the check box to discover certificates along with private keys. If the device has many certificates, this may take a bit longer.
Private Key Default Password	Enter the default password.

8. Enter the field information in the **Secondary device information** section as follows:
   - **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
   - **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
   - **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

> **Note:**
> - By clicking the **Add** button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
> - By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

9. Click the **Save** button to add a Firewall device.

> **Note:** To discard the changes, click the **Cancel** button.

A pop-up message is displayed as **Device added successfully**.

CLI Commands

Minimum required permissions

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Version of device:** 6.x or above
- **License type:** Cert+ Only 16
- **Device management**

  Network > Configuration > Read Only (Communication and version check)

- **Certificate discovery**
  - System > Configuration > Read/Write (System Local Certificates, System Setting)
  - VPN > Read (VPN Profiles)
  - Firewall > Others > Read (SSL/SSH Inspection Profile)
  - User & Device > Read (User Authentication Setting Profile)
- **Certificate Push and Bind**
  - System > Configuration > Read/Write (Push to System Local Certificates, Bind System Server Certificate)
  - VPN > Read/Write (Bind to VPN Setting Profile, VPN Ipsec profile)
  - Firewall > Others > Read/Write (Bind to SSL/SSH Inspection Profile)
  - User & Device > Read/Write (Bind to User Authentication Setting Profile)

Operation	Command	Description
System Status	`get system status`	Displays system information such as firmware version, VDOM status, and system mode.
Configure VDOM	`config vdom`	Enters VDOM configuration mode to manage Virtual Domains.
Edit configurations	`edit ?`	Enters edit mode for a specific configuration object (e.g., VDOM, interface, etc.).
End	`end`	Ends the current configuration mode and applies changes.
Switch to global	`config global`	Switches to the global configuration context.
Configure System's console	`config system console`	Used to configure console settings; often used with set output standard for terminal output.
Set output to standard	`set output standard`	Sets the console output format to standard (non-JSON or non-table).
Show full CA certs (VPN)	`show full-configuration vpn certificate ca`	Displays full configuration of CA certificates used in VPN.
Show full CA certs	`show full-configuration certificate ca`	Displays full configuration of CA certificates in the system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description
Show full local certs (VPN)	`show full-configuration vpn certificate local`	Displays full configuration of local VPN certificates.
Show full local certs	`show full-configuration certificate local`	Displays full configuration of local certificates in the system.
Show IPSec VPN config	`show vpn ipsec {CONFIGURATIONS}`	Displays IPsec VPN configurations.
Show SSL VPN settings	`show vpn ssl settings`	Displays current SSL VPN settings.
Show user settings	`show user setting`	Displays user authentication settings.
Show SSL/SSH profiles	`show firewall ssl-ssh-profile`	Displays SSL/SSH inspection profiles used in firewall policies.
List CA cert names (VPN)	`show full-configuration vpn certificate ca ?`	Lists available CA certificate names in VPN configuration.
List CA cert names	`show full-configuration certificate ca ?`	Lists available CA certificate names in the system configuration.
List local cert names (VPN)	`show full-configuration vpn certificate local ?`	Lists available local certificate names for VPN.
List local cert names	`show full-configuration certificate local ?`	Lists available local certificate names configured on the device (non-VPN).
Set CA certificate	`set ca \"{CERT_CONETNT}\"`	Sets the CA certificate content during certificate configuration.
Set private key	`set private-key \"{PVT_KEY_CONETNT}\"`	Sets the private key content for a certificate.
Set certificate content	`set certificate \"{CERT_CONETNT}\"`	Sets the actual certificate content.
Set password	`set password`	Sets a password (often used when importing password-protected keys/certs).
Unset password	`unset password`	Removes a previously set password from the configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description
Configure SSL VPN settings	`config vpn ssl settings`	Enters configuration mode for SSL VPN settings.
Unset SSL VPN cert	`unset servercert`	Removes the currently configured SSL VPN server certificate.
Set SSL VPN cert	`set servercert {CERT_NAME}`	Sets the server certificate for SSL VPN.
Configure SSL/ SSH profile	`config firewall ssl-ssh-profile`	Enters configuration mode for SSL/SSH inspection profiles.
Unset SSL/SSH cert	`unset server-cert`	Removes the configured certificate from the SSL/SSH profile.
Set SSL/SSH cert	`set server-cert {CERT_NAME}`	Sets the server certificate for SSL/SSH inspection.
Configure global settings	`config system global`	Enters system-wide global configuration mode.
Set admin portal cert	`set admin-server-cert {CERT_NAME}`	Sets the certificate used for the FortiGate admin GUI (HTTPS portal).
Configure user settings	`config user setting`	Enters configuration mode for user authentication settings.
Set user auth cert	`set auth-cert {CERT_NAME}`	Sets the certificate used for user authentication.
Configure IPsec VPN	`config vpn ipsec`	Enters IPsec VPN configuration mode.
Append cert to IPsec VPN	`append certificate {CERT_NAME}`	Appends a certificate to the IPsec VPN configuration.
Generate certificate	`execute vpn certificate local generate`	Generate a local certificate on the device.

Pushing Server Certificates to the Device

The certificate can be pushed to the device in only PEM format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Starting from FortiOS version 5.4 and above, when pushing a certificate to FortiGate, if a certificate with the intended name is already present, a timestamp is automatically appended to the certificate name. This ensures the new certificate is successfully imported without conflict, while retaining the original.

Warning:

FortiGate does not allow importing a certificate that has already been imported earlier—even if you attempt to import it again under a different name or context. FortiOS maintains a checksum or fingerprint of certificates.

If a certificate with the same cryptographic material already exists in the system (for example, with the same subject, serial number, and public key), it will reject duplicates to prevent redundancy or configuration conflicts.

Profiles will be discovered irrespective of the cert sync option selected during device addition or during an on-demand discovery. The following profiles will be discovered currently in AppViewX:

- **Shared location:** Denotes a push-only operation which pushes a certificate to the end device.

  Profile convention : {DeviceName}::System/Vdom name

- **SSL VPN Settings:** SSL VPN allows remote users to securely connect to the corporate network using an encrypted SSL tunnel via a web portal or FortiClient. Apushed certificate can be associated to SSL-VPN setting if it is enabled.

  Profile convention : {DeviceName}::System/Vdom name::SSL VPN Setting:SSL VPN Setting

- **SSL/SSH Inspection Profile:** SSL/SSH inspection profiles inspect encrypted traffic (HTTPS/SSH) for threats or policy enforcement. Apushed certificate can be associated to any inspection profile if it is configured with Protecting SSL Server option.

  Profile convention : {DeviceName}::System/Vdom name::SSL/SSH Inspection Profile:{Inspection profile name}

- **System Setting Https Server Certificate:** This controls which certificate is used to secure access to the FortiGate administrative web interface. Apushed certificate can be associated to the System administration setting server certificate.

  Profile convention : {DeviceName}::System::System Setting Https Server Certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **User Authentication settings:** Defines how users authenticate to FortiGate (e.g., captive portal, VPN, web portal). Ensures only clients with valid certificates can authenticate, enhancing security. Apushed certificate can be associated to the User authentication setting server certificate.

  Profile convention : {DeviceName}::System:User Authentication settings:User Authentication settings

- **IPSec VPN Profile:** IPSec VPN allows site-to-site or remote client VPN connections using the IPSec protocol suite. Apushed certificate can be associated to the IpSec tunnel configured in the device.

  Profile convention : {DeviceName}::System:IPSec VPN Profile:{TUNNEL_NAME}

Backing Up Certificates

Before a bind operation, a backup will be taken for the currently associated certificate so that a rollback can be performed once the new certificate is associated.

Binding Certificates

Certificates can be bound for profile connectors. These connectors include all the connectors other than the shared location connector.

The selected selected certificate will be pushed to the shared location first and then the certificate will be associated to the selected profile.

Rolling Back Certificates

In the event of a rollback, the system restores the previous state by unbinding the current certificate, pushing and binding the backed-up certificates to the selected profile.

CSR Generation

Note: Generation of CSR can be performed for a FortiGate device during certificate enrollment. The Partition name, CSR File Name, and Key File Name have to be provided.

Minimum Privileges required in FortiManager

JSON API Access

Required for JSON API operations, it enables AppViewX to communicate with FortiManager through REST API calls. (`System Settings -> Administrator -> Edit Administrator`).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Required access: Read/Write

System Settings Access

Required to manage system certificates and configurations. (System Settings > Admin Profiles > Edit Administrator)

Required access: Read/Write

Configuring FortiManager Firewall Device

To add a FortiManager device:

1. Go to (**Menu**) > **CERT+** > **Device Management**.
   By default, the **ADC** tab opens.
2. Select the **Firewall** tab.
3. Click the + (**Add**) icon located on the top right corner.
   The **Add** page appears.
4. Select the **Fortinet** vendor from the left side bar.
5. Enter the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select **FortiManager**.
***Device name**	Unique custom identifier of your device.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Data center	The data center on which the device has been hosted. Select a datacenter from the dropdown list or enter a data center name.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
***SSH Port**	By default, it is 22.
***HTTPS Port**	By default, it is 443. **Note:** Any change in port configuration is captured in audit logs.
**: Mandatory fields*	

6. Enter the field information in the **Credentials** section:

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **Credential List - AppViewX** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. • If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential Type from the dropdown list. If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your password can be of any length with a combination of alpha-numerical, symbols, and special characters.
**: Mandatory fields*	

7. Enter the field information in the **Secondary device information** section as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
- **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
- **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Note:
- By clicking the **Add** button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing, and management can be seamlessly handled in AppViewX.

8. Click the **Save** button to add a Firewall device.

Note: To discard the changes, click the **Cancel** button.

A pop-up message is displayed as **Device added successfully**.

Discovering Certificates

- Discovery (on-demand and scheduled) of certificates from the FortiManager certificate repository including:
  - Local certificates
  - Local CA certificates
- The system creates the following certificate profiles with correct naming conventions:

Certificate Profile	Naming Convention
System Local	`deviceName::FortiManager::System`
HTTPS & Web Service	`deviceName::FortiManager::System::AdminServerCertificate`
SAML SSO IdP (when enabled)	`deviceName::FortiManager::System::SamlIdp`
HA Cluster	`deviceName::FortiManager::System::HA`

- When config sync is triggered and cert sync is enabled, the system automatically:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Initiates certificate discovery
- Creates/updates corresponding profiles
- Maintains the association between certificates and profiles

> **Note:** Certificates from FortiGate devices managed by FortiManager are currently not supported in this integration.

- Frame application connectors for the server certificates based on the profile it was discovered from. (Default connector is overridden by Profile connectors.)

Pushing Server Certificates to the Device

> **Note:** The certificates can be pushed to the FortiManager device only in **PEM** format.

Parameters

- **Certificate File Name**: Mandatory parameter specifying the name for the certificate file on the device

Push Root and Intermediate Certificates

- **Functionality**: Root and intermediate certificates can be included with the server certificate during push operation
- **Import Behaviour**:
  - Server certificate imported to **local cert** store
  - Trust certificates (root/intermediate) imported to **local ca cert** store

File Naming Requirements

- File name is **mandatory** for all certificates in the chain.
- Each certificate in the chain requires a unique file name.
- If any of the specified names already exists on the device, the push operation will **fail**
- **Overwrite Option**: Can be resolved by checking the **overwrite** option to replace existing certificates
- **Private Key In Device option**: Used to map certificate to a CSR file in FortiManager. When selected, the CSR file in the device will be updated with the certificate content.

Trust Certificate Push

All trust certificates will be imported to the local ca certificate store on the FortiManager device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Naming and Override Behavior

- Same file naming requirements apply as server certificate push.
- Mandatory file names for all trust certificates being pushed.
- Push operation fails if certificate names already exist on device.
- **Overwrite Option:** Available to replace existing trust certificates with the same names.

Binding Certificates

Certificates can be bound to profile connectors in FortiManager. Certificate binding is supported for the following profiles:

- Admin Server Certificate
- SAML Identity Provider
- High Availability (HA)

After the push operation, the certificate will be referenced using the pushed certificate name in the FortiManager configuration. This ensures proper association between the certificate and the specific profile functionality.

Backing Up and Rolling Back Certificates

Backup and rollback operations are not supported because FortiManager does not expose the private key content of the server certificates. Therefore, it is not possible to backup or restore the previous state of the certificates in case of a rollback.

CSR Generation

The FortiManager CSR generation feature allows users to create Certificate Signing Requests (CSR) directly on FortiManager devices through SSH connectivity.

Note: Command Format: execute certificate local generate [filename] [bitlength] [commonname] [country] [state] [locality] [organization] [organizationunit] [email]

Parameters

- **CSR File Name**: Mandatory parameter specifying the name for the CSR file on the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Once CSR generation is successful and signed certificate is received from CA, the certificate has to be pushed back to the device with the same CSR file name with PrivateKeyInDevice option selected to map the certificate correctly.

Note:

- Implementation supports only RSA key generation; no support for EC/DSA or any other key type.
- Supported bit lengths for RSA key type: 512, 1024, 1536, 2048, 3072, 4096

CLI Commands

CSR generation

1. Generate CSR in the device:

```
execute certificate local generate <name> <key_size> <CN> <C> <ST> <L> <O> <OU>
    <email>
```

2. Get CSR file content : `show system certificate local <csr_file_name>`

APIs

`POST https://$HOST:$HTTPS_PORT/jsonrpc`: This is the standard format of the API URLs triggered in FortiManager for all the use cases.

Standard payload format:

```
{
 "id": <id>,
 "method": "<method, could be exec, add, update>",
 "params": [
    {
       "url": "URL for the request",
       "data": {
          <Data required for the request>
       }
    }
 ],
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 "session": <session_id>
}
```

Operation	Method	URL	Data	Description
Login using json rpc	exec	/sys/login/user	{ "user": {USER_NAME}, "passwd": {PASSWORD} }	A login operation is required in order to get a session ID.
System Status	get	/cli/global/system/status	{ }	Displays system information such as firmware version and system mode.
Show local certs	get	/cli/global/system/certificate/local	{ }	Displays full configuration of local server certificates. (Private key of the certificates are masked in the response).
Show local CA certs	get	/cli/global/system/certificate/ca	{ }	Displays full configuration of local CA certificates in the system.
Show system	get	/cli/global/system/admin/setting	{ }	Displays the system

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Method	URL	Data	Description
admin settings				admin setting details.
Show HA settings	get	/cli/global/system/ha	{ }	Displays the HA setting details.
Show SAML Idp settings	get	/cli/global/system/saml	{ }	Displays the SAML Idp setting details.
Add/Update local server certificate	add/update	/cli/global/system/certificate/local	{ "certificate": "{CERTIFICATE_CONTENT}", "name": "{CERTIFICATE_FILE_NAME}", "private-key": "{PRIVATE_KEY_CONTENT}" }	To import a server certificate with a private key to local store.
Add/Update local CA certificate	add/set	/cli/global/system/certificate/local/ca	{ "certificate": "{CERTIFICATE_CONTENT}", "name": "{CERTIFICATE_FILE_NAME}" }	To import a trusted CA certificate to local ca store.
Modify system admin server certificate	update	/cli/global/system/admin/setting	{ "admin_server_cert": "{CERTIFICATE_FILE_NAME}" }	To modify the admin server certificate mapped to the FortiManager UI portal.
Modify HA certificate	update	/cli/global/system/ha	{ "local-cert": "{CERTIFICATE_FILE_NAME}" }	To modify certificate mapped to the HA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Method	URL	Data	Description
Modify SAML Idp certificate	update	/cli/global/system/saml	`{ "cert": "{CERTIFICATE_FILE_NAME}" }`	To modify certificate mapped to the SAML Idp setting.

Troubleshooting

Device goes to unresolved state after onboarding

The device might enter an unresolved state due to connectivity issues from the AppViewX installed node or CC node. In such cases, follow these steps:

- Attempt to establish an SSH connection from the AppViewX installed node or CC node to the FortiManager server.
- Verify if there is proper connectivity between the nodes and the FortiManager server. Check for the JSON API access provided for the user onboarded in AppViewX.

Device addition with FQDN fails when using external vault

When adding a firewall device with FQDN in AppViewX, the credentials are fetched from the external vaults via device FQDN. A dot (.) is automatically added at the end of the FQDN for firewalls in AppViewX during the credential lookup process.

Note:

- The credentials configured in the external vault must have a dot (.) at the end of the FQDN to match the lookup pattern used by AppViewX.
- If the FQDN of the device is `test.avx.com`, then the credential entry in external vault should be configured as: `test.avx.com.`

Validating the Device

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to **Menu** > **CERT+** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click the **Firewall** tab.
3. Search the device name and validate whether the device is added successfully.

Adding Juniper Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port number 22 (SSH)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Not supported

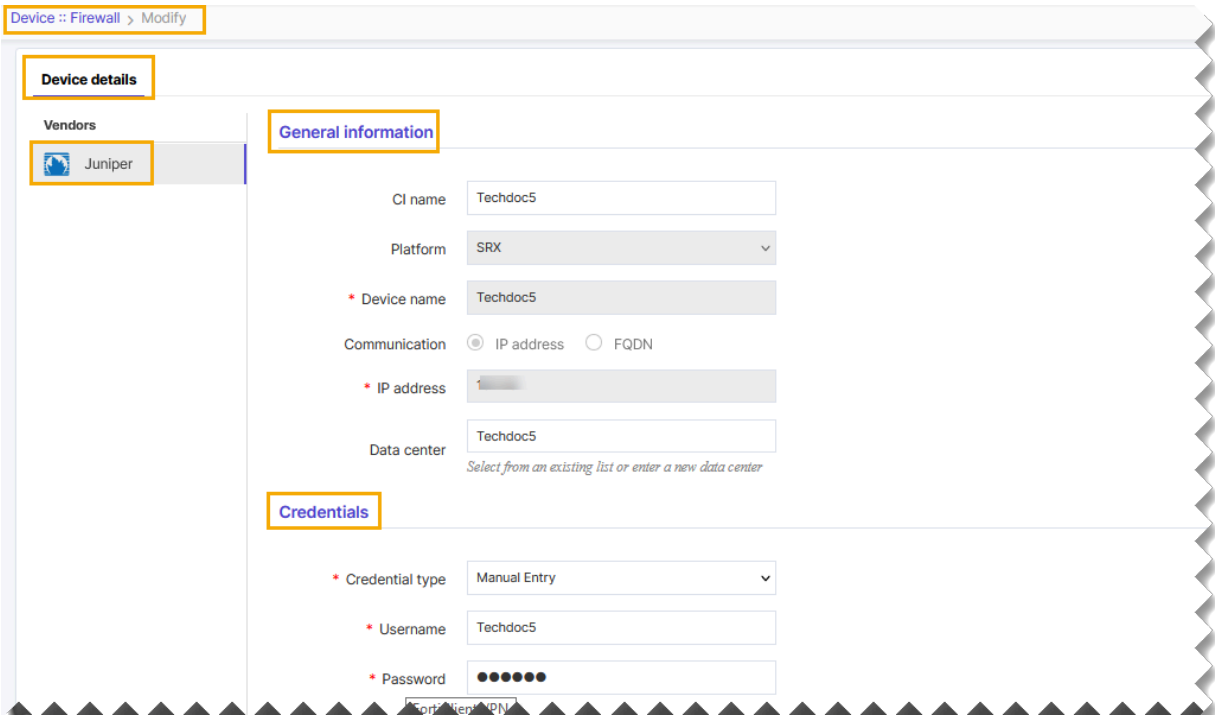
Note: For Visual Workflow action items, you will require credentials with write privilege.

Configuring a Juniper Firewall Device

To add a Juniper device,

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Firewall**.
3. On the **Device :: Firewall** page, click (**Add**).
   The **Device :: Firewall > Add** page is displayed.
4. Select the **Juniper** vendor from the left side bar. bar.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • SRX.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

6. Enter or select the field information in the **Credentials** section:

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the password.
**: Mandatory fields*	

7. Enter or select the field information in the **Secondary device information** section as follows:

   - **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
   - **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
   - **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

   Note:
   - By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
   - By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

8. Click the **Save** button to add an Firewall device.

   Note:
   - To discard the changes, click the Cancel button.

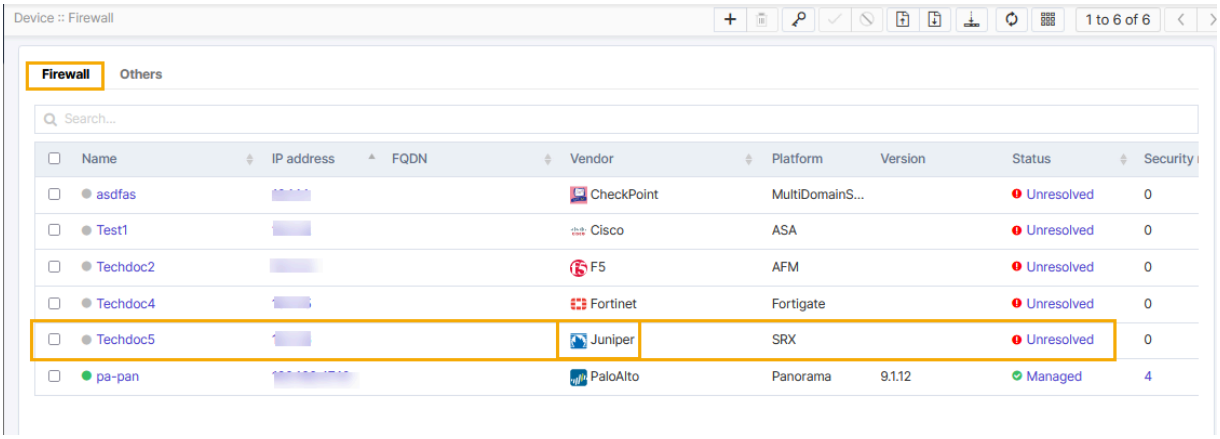
   A pop-up message is displayed as **Device added successfully**.

Validating a Juniper Firewall Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Firewall**.
   The **Device :: Firewall** page is displayed. This page is an inventory of all the existing firewall devices.
3. Search the device name and validate whether the device is added successfully.



What's Next

Once you configured the Juniper firewall, you are ready to proceed with the following action to enable the auto enrollment:

- Automating Certificates for Firewall Devices in AppViewX

Adding Palo Alto Firewall Device

Refer to Automating CLM for Palo Alto.

Deleting a Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Delete**) icon in the command bar.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Delete** confirmation popup window is displayed.

5. Click **Yes**.
   The firewall will be removed from the device inventory.

Importing a Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Import**) icon in the command bar.
   You will be redirected to the import firewall page.
5. Download the sample <.csv> or <.xls> file.
6. Update the details.
7. Click the browse and upload button.
8. Upload the files.
   Firewall details will be updated to the firewall inventory.

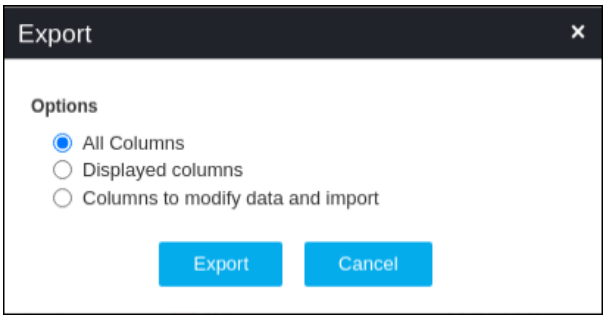
Exporting a Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name. If you are exporting details of multiple firewalls, select the check-boxes for each one.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Export**) icon in the command bar at the upper right of the screen.
5. On the Export pop-up screen that is displayed, select the type of information you want to export and click the **Export** button.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



a. **All Columns** - Select this option if you want to export all information about the firewall.
b. **Displayed columns** - Select this option if you want to export only the information that is visible on the firewall screen.
c. **Columns to modify data and import** - Select this option if you are exporting firewall details to make modifications and then re-import the data into the firewall Inventory.

6. On the screen that opens, select the location where you want the firewall details file to go, then click **Save**.
   Firewall details will be downloaded as an Excel `<.xls>` file.

Managing a Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. To start managing the firewall, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   • Config fetch will be triggered and the firewall will get managed.
   • Firewall status is changed to **Manage** in Firewall inventory.

Unmanaging a Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation popup message that is displayed.
   Firewall device status is changed to UnManaged in Firewall inventory.

Executing a Fetch Config for Firewall

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Firewall** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the firewall.** The configuration will be fetched from the server.

Configuring Switches

Prerequisites

- Beyond trust PAM must be integrated with AppViewX for managing the device credentials.
- Network devices must be managed in AppViewX for workflow to be executed.

You can configure Arista, Cisco or Juniper switches using these instructions.

To configure a router:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Switch** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter the fields in the respective sections as described:

Field Description of Switch

Field	Description
General Information	
***Switch type**	Select between L2 and L3. By default, L2 is selected.
***Device name**	Unique custom identifier of your device.
***IP address**	Enter the IP address based on the selected communication mode.
***Port**	Enter the port details. By default, it is 22.
Model	Enter the switch model.
Device description	Provide a description for the switch.
Data center	Enter a data center.
Credentials	
***Credential type**	Select the credential type from the dropdown: • **Manual entry (default):** The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **Credential List - AppViewX:** The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication.
Secondary device information	
Peer device	By default, **Manual Entry** is not selected. Select this checkbox if you want to add another switch.
The following fields appear if the **Manual Entry** checkbox is selected.	
***Switch type**	Select between L2 and L3. By default, L2 is selected.
***Device name**	Unique custom identifier of your secondary device.
***IP address**	Enter the IP address of the secondary device.
***Port**	Enter the port details. By default, it is 22.
Model	Enter the switch model.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Device description	Provide a description for the switch.
Data center	Enter a data center.
Secondary device credentials	
***Credential type**	Select the credential type from the dropdown: • **Manual entry (default):** The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **Credential List - AppViewX:** The username and password can be saved to a list and referenced when adding the device. The credential lists are integrated within AppViewX application for the secured authentication.
Enable Password	Enter a password.
*Fields marked with asterisk (*) symbol are mandatory.	

4. Click **Save.**
   A message, *Device is added successfully,* appears.

What to do next

Once the credentials are updated a fetch configuration should be initiated in the AppViewX node to check if the credentials are working and if whether all the devices are in managed state. See Manually Fetch the Configuration for a Device.

For other device-related actions, see Inventory Actions.

Configuring Routers

You can configure Cisco or Juniper routers using these instructions.

To configure a router:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Router** tab.
3. Enter the fields in the respective sections as described:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description of Router

Field	Description
General Information	
***Device name**	Unique custom identifier of your device.
***IP address**	Enter the IP address based on the selected communication mode.
***Port**	Enter the port details. By default, it is 22.
Model	Enter the router model.
Device description	Provide a description for the router.
Data center	Enter a data center.
Credentials	
***Credential type**	Select the credential type from the dropdown: • **Manual entry (default):** The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **Credential List - AppViewX:** The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication.
Secondary device information	
Peer device	By default, **Manual Entry** is not selected. Select this checkbox if you want to add another router.
The following fields appear if the **Manual Entry** checkbox is selected.	
***Device name**	Unique custom identifier of your secondary device.
***IP address**	Enter the IP address of the secondary device.
***Port**	Enter the port details. By default, it is 22.
Model	Enter the router model.
Device description	Provide a description for the router.
Data center	Enter a data center.
Secondary device credentials	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Credential type**	Select the credential type from the dropdown: • **Manual entry (default):** The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **Credential List - AppViewX:** The username and password can be saved to a list and referenced when adding the device. The credential lists are integrated within AppViewX application for the secured authentication.
Enable Password	Enter a password.
*Fields marked with asterisk (*) symbol are mandatory.	

4. Click **Save.**
   A message, *Device is added successfully,* appears.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to (**Menu**) > **CERT+** >**ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Switch** tab.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

What to do next

Once the credentials are updated a fetch configuration should be initiated in the AppViewX node to check if the credentials are working and if whether all the devices are in managed state. See Manually Fetch the Configuration for a Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For other device-related actions, see Inventory Actions.

Configuring and Managing Cloud Devices

- Viewing the Cloud Device Inventory
- Amazon Web Services (AWS)
- Azure
- Google Cloud Platform (GCP)
- Apache SSM integration specification
- Functional Specification
- Generic Linux SSM Integration Specification
- Instances Discovery Specification
- Delete Cloud
- Import Cloud
- Export Cloud
- Manage Cloud
- Unmanage Cloud
- Fetch Config for Cloud

Viewing the Cloud Device Inventory

The cloud device inventory is displayed at two levels:

- Outer inventory: Displays details of all cloud accounts added
- Inner inventory: Displays details of an individual cloud account

To access the outer cloud device inventory:

1. In the AppViewX UI, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
   The **Device** :: **ADC** page is displayed.
2. From the **Device :: ADC** screen, select **Cloud**.
   The **Device :: Cloud** outer cloud device inventory is displayed.

   The fields displayed in the inventory are explained in the table below:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: The order in which these fields are displayed in the inventory can vary depending on the value selected from the **Vendor** dropdown list.

Field	Description
Vendor	From this dropdown list, select a vendor to filter the cloud device inventory as required.
Account Name	Name of the account to which the cloud device belongs
Account Description	Applicable only for a child account, this field displays the following details: • Account type (child) • Master account number • Discovery type: **ROLE_BASED** or **ORGANIZATION_BASED**
Vendor	Cloud device vendor name
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for organizations. For organizations, the resource discovery status is set to **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field indicates the status of the resource discovery for the individual entities belonging to a discovered project using the following values: • **Not started**: Resource discovery by AppViewX is yet to begin **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery by AppViewX in the customer's GCP environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's GCP environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX in GCP. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • for ACM and ELB resources • for all existing devices and projects as part of data migration
Cert Discovery Status	**Note:** Cert discovery status is not applicable for organizations. For organizations, the cert discovery status is set to **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: The certificate discovery status of accounts in this outer cloud inventory list depends on the corresponding status of all their reporting entities listed in the project level inventory.
	
	Indicates the status of the certificate discovery for the discovered projects using the following values:
	• **Not started**: Certificate discovery for the project is yet to begin
	
	Note: At this point, the resource discovery status of the associated project can be **Not started**, **In-Progress**, or **Completed**.
	
	• **In-Progress**: Certificate discovery by AppViewX in the customer's GCP environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all projects is either **Completed** or **Not Applicable**.
	• **Completed**: Certificate discovery by AppViewX in the customer's GCP environment is complete.
	
	Note: This is possible only when the certificate discovery status for all the entities associated with the project is **Completed**.
	
	• **Not Applicable**: The certificate discovery status is set to **Not Applicable**:
	  • for EC2 when no EC2 instances are discovered
	  • for all existing devices and child projects as part of data migration
	
	Note: The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.

Project ID	**Note:** This field is displayed only when **Vendor** = **GCP Projects**. User-assigned unique identifier of the project
Project Number	System-generated unique identifier of the project assigned by GCP

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Project Name	User-friendly name assigned to the project

Note: Alternate steps to access the cloud device inventory:

a. In the AppViewX UI, go to (**Menu**) > **Platform** > **ASSET MANAGEMENT** > **Device Inventory**.

The **Device :: ADC** page is displayed.

b. From the **Device :: ADC** screen, select **Cloud**.

The **Device :: Cloud** outer cloud device inventory is displayed.

Amazon Web Services (AWS)

AWS (Amazon Web Services) is a comprehensive cloud computing platform provided by Amazon. It offers a wide range of cloud services, including computing power, storage options, networking, machine learning, and database services.

- Onboarding a Standalone Account
- Onboarding a Cross Account in AppViewX
- AWS Standalone Account Onboarding via Cross Account

AWS Services Supported by AppViewX

AppViewX supports the following AWS services:

- **ACM**

  AWS Certificate Manager (ACM) is a service provided by Amazon Web Services that simplifies the process of provisioning, managing, and deploying SSL/TLS certificates for use with AWS services and your internal connected resources.

- **IAM**

  IAM (Identity and Access Management) is a web service that helps you securely control access to AWS resources. IAM enables you to manage users, groups, roles, and their associated permissions to ensure that the right individuals and services have the appropriate access to your AWS resources.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **ELB**

  Elastic Load Balancer, ELB, is a service that automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in one or more Availability Zones. ELB helps ensure the availability, scalability, and fault tolerance of your applications.

  AWS provides three types of load balancers:

  - **Application Load Balancer** (**ALB**): Best suited for HTTP and HTTPS traffic, providing advanced request routing features targeted at the delivery of modern application architectures, including microservices and containers.
  - **Network Load Balancer** (**NLB**): Designed to handle millions of requests per second while maintaining ultra-low latencies, best suited for TCP, UDP, and TLS traffic where extreme performance is required.

  Classic Load Balancer (**CLB**): Provides support for basic load balancing of HTTP/HTTPS and TCP/SSL traffic
- **CloudFront**

  CloudFront is a Content Delivery Network (CDN) service. It speeds up the delivery of your web content by caching copies of your content at edge locations around the world.
- **EC2**

  Amazon EC2 (Elastic Compute Cloud) is a web service provided by Amazon Web Services (AWS) that offers resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers by providing a secure, resizable, and flexible

Onboarding a Standalone Account

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: The following steps cover only the bare minimum requirements for onboarding a standalone AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Note: If you already have a AWS account set up with the required roles and policies created and mapped, refer the instructions for **Onboarding a Standalone Account in AppViewX**.

Prerequisites for Onboarding a AWS Standalone Account in AppViewX

- An IAM role must be created in your AWS account with the required roles and policies created and mapped. For instructions, refer the documentation here.

  Note: For additional AWS documentation for creation a standalone account, refer to the links in the **References** section.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

    Important: For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important: AWS standalone device migration is supported only from the following versions of CERT+ SaaS: **v2020.1**, **v2020.2**, **v2020.3** - **v2020.3 FP7**. The following prerequisites are also applicable to only these versions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Important: AWS device migration **is not** supported from the following versions of CERT+ SaaS: **v2012.x**, **v2019.x**, and **v2021.x**. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Note: For customers migrating from versions **20.1.x**, **20.2.x**, and **20.3.6**, AppViewX recommends that you delete the following before migration:

- All of their Amazon CA settings
- Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).

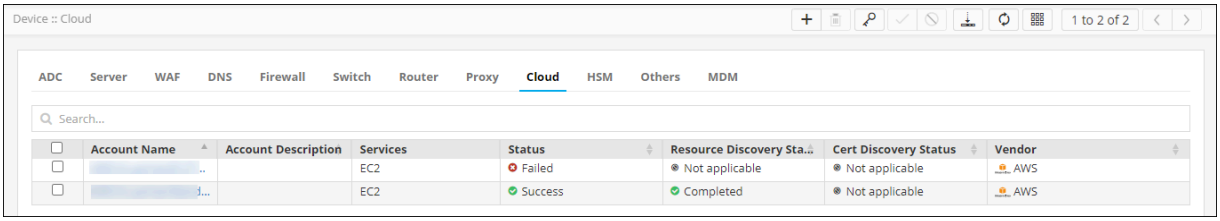
Note: For customers migrating from version **v2020.3.10** (mandatory):

- Delete all of their Amazon CA settings before migration.
- Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the **standalone AWS cloud accounts** migrated from the above listed versions to version **v2022.1 FP1**:

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
   The **Device :: Cloud** page is displayed.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

> **Troubleshooting:** If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.

4. From the top-right corner of the **Device :: Coud** page, click the (**Fetch config**).
   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

> **Note:** For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

Before Migration

Merge permissions from all individual buckets into any one S3 bucket.

After Migration

1. Select a migrated standalone account from the **Device :: Cloud** page.
   The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
4. Click **Add**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **Save**.
   Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

AWS IAM Prerequisites for Standalone Account Onboarding

For Discovering and Managing SSL Certificates in ACM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "acm:GetCertificate",
        "ec2:DescribeRegions",
        "acm:ListCertificates",
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate",
        "acm:ListTagsForCertificate",
        "acm:RemoveTagsFromCertificate"
      ],
      "Resource": "*"
    }
  ]
}
```

For Discovering and Managing SSL Certificates in CloudFront

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "Action": [
                "iam:GetServerCertificate",
                "acm:GetCertificate",
                "acm:ListCertificates",
                "iam:ListServerCertificates",
                "ec2:DescribeRegions",
                "cloudfront:ListDistributions",
                "acm:ImportCertificate",
                "acm:AddTagsToCertificate",
                "acm:ListTagsForCertificate",
                "acm:RemoveTagsFromCertificate",
                "cloudfront:UpdateDistribution",
                "cloudfront:GetDistributionConfig",
                "cloudfront:ListTagsForResource",
                "iam:UploadServerCertificate",
                "iam:ListServerCertificateTags",
                "iam:TagServerCertificate",
                "iam:UntagServerCertificate"
            ],
            "Resource": "*"
        }
    ]
}
```

For Managing SSM Permissions for the EC2 Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
    "ssm:DescribeDocument",
    "ec2:DescribeInstances",
    "s3:ListAllMyBuckets",
    "ssm:DescribeInstanceInformation",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "ssm:GetDocument",
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
          ],
          "Resource": "*"
      }
   ]
}
```

For Managing SSM Permissions for EC2 Role

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "ssm:DescribeDocument",
            "ec2messages:GetEndpoint",
            "ec2messages:GetMessages",
            "ssmmessages:OpenControlChannel",
            "ec2messages:DeleteMessage",
            "ssm:UpdateInstanceInformation",
            "ec2messages:FailMessage",
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
         ],
         "Resource": "*",
         "Effect": "Allow"
      },
      {
         "Action": [
            "s3:PutObject",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

For Enabling S3 Bucket Access to AppViewX

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
  "s3:ListBucket",
  "s3:DeleteObject",
  "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::appviewx-s3/*",
        "arn:aws:s3:::appviewx-s3"
      ],
    }
  ]
}
```

For Discovering and Managing SSL Certificates in ELB

```
{
  "Version": "2012-10-17",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "elasticloadbalancing:ModifyListener",
        "ec2:DescribeInstances",
        "iam:ListServerCertificates",
        "elasticloadbalancing:DescribeTags",
        "ec2:DescribeRegions",
        "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
        "iam:UploadServerCertificate",
        "iam:ListServerCertificateTags",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "ec2:DescribeAvailabilityZones",
        "acm:GetCertificate",
        "elasticloadbalancing:DescribeTargetHealth",
        "acm:ListCertificates",
        "elasticloadbalancing:DescribeTargetGroups",
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate",
        "acm:ListTagsForCertificate",
        "acm:RemoveTagsFromCertificate",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:DescribeListenerCertificates"
      ],
      "Resource": "*"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For Discovering and Managing Certificates in IAM

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
            "iam:ListServerCertificates",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "ec2:DescribeRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

For Discovering and Managing Private CA Certificates

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "acm:RenewCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "acm-pca:CreateCertificateAuthorityAuditReport",
 "acm-pca:DescribeCertificateAuthorityAuditReport,
 "acm-pca:GetCertificate",
 "acm-pca:ListCertificateAuthorities",
 "acm-pca:IssueCertificate",
 "acm-pca:RevokeCertificate",
 "s3:GetBucketLocation",
 "s3:GetObject"
        ],
        "Resource": "*"
    }
  ]
}
```

Onboarding a Standalone Account in AppViewX

The following instructions will guide you through the process of onboarding a standalone account in AppViewX for the supported AWS services (listed and explained here):

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, select **Standalone**.
***Account name**	Enter your AWS account name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	According to the type of the new cloud device being added, select the corresponding Amazon Cloud Service for the device.
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Service region*	Service regions are regions that are supported by the selected service. From the dropdown list, select the service regions that should be scanned for certificates. **Note:** To be able to fetch and select from the available regions, ensure that the credentials have been provided in the **Credentials** section.
CA Operation Mode*	**Note:** This field is displayed only when the **Amazon Private CA** service is selected. From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • **ACM** • **PCA**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
S3 Bucket*	**Note:** This field is displayed only when the **PCA** CA operation mode is selected. Enter the S3 bucket name.
Discovery Certificate	**Note:** This field is displayed only when one/both of the CA operation modes are selected. To enable instance certificate discovery at the time of device addition, select this checkbox.
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

What's Next?

After you have successfully onboarded a standalone account in AppViewX, the next step is to discover existing certificates for the onboarded account and/or enroll new certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

- Create an IAM user in your AWS account.
- Create access keys for the root user.
- Create IAM policies using the JSON editor.
- Accessing member accounts.
- Using IAM roles for Amazon EC2 instances.
- Define custom IAM permissions for customer managed policies.

Onboarding a Cross Account in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

This section of the documentation will guide you through the process of onboarding an AWS cross account in AppViewX.

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Note: If you already have a AWS account set up with the required roles and policies created and mapped, you can directly start with **Onboarding a Cross Account in AppViewX** .

Prerequisites for Onboarding a AWS Cross Account in AppViewX

- Ensure that the following configurations are done on the AWS Management Console:
  - In your AWS master account:
    1. Create an IAM user in the AWS master account.
    2. Generate user identity.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Attach policies to the created user.

   For the AWS IAM permissions to be added for the master account, click here.

- In your AWS child account:
  1. Create a role in the child account in AWS.
  2. Attach policies to the created role.

     For the AWS IAM permissions to be added for the child account, click here.

  3. Create an EC2 role. This will be used to manage the existing EC2 instance in the AppViewX device inventory.
  4. Attach policies to the EC2 role.

     For the AWS IAM permissions for the EC2 policy, click here.

     For the AWS IAM permissions for the EC2 role, click here.

- If account specific S3 buckets have been deployed for EC2 integration, ensure that the bucket names are suffixed with the corresponding account number.

  For instruction on creating an S3 bucket in your AWS account, see References.

> **Note:** For detailed instructions, you can access the corresponding AWS documentation using the references given here.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

    > **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Onboarding a Cross Account in AppViewX

In AWS, cross-account discovery can be set up in two ways:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Organization-based**: A centralized discovery mechanism that automatically finds and accesses resources across accounts in your AWS Organization using built-in trust and roles
- **IAM Policy-based**: A more flexible discovery mechanism that allows to connect to only the required accounts by manually configuring roles and permissions

Onboarding a Cross Account in AppViewX for Organization-based Discovery

The following instructions will guide you through the process of onboarding a standalone account in AppViewX for the supported AWS services (listed and explained here):

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	To onboard a cross account for organization-based discovery: a. Select **Organization Based Discovery**. The **Organization based Discovery** dialog box is displayed. b. Enter/Select the details required to configure organization-based discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Policy Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the services required for the CLM operations. **Tip:** To select all services, select the **Select all** check box displayed at the beginning of the list of services. **Note:** • When **ACM (Certificate Authority)** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Certificate Authority Service**to configure the ACM services. These fields are explained in the table in Step 10. • When **Amazon Private CA** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Private CA**. These fields are explained in the table in Step 11. • When the **EC2(EC2 Instance)** service is selected, an additional set of fields is displayed to configure the EC2 services. These fields are explained in the **EC2 Services** table in Step 7.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **ACM Certificate Authority Service** section.

> **Note:** This section is displayed only when one or both **ACM** services are selected from the **Services** dropdown list.

Field description for the ACM Certificate Authority Service

Field	Description
Role Setting Preference*	**Note:** This field is displayed only when both auto discovery modes (**Organization Based Discovery** and **IAM Policy Based Discovery**) are selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select one of the following options: • **Organization Based Discovery** • **IAM Policy Based Discovery**
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle.
**: Mandatory fields*	

9. Enter/Select the required details in the **ACM Private CA** section.

> **Note:** This section is displayed only when the **ACM (Amazon Private CA)** service is selected for a **Cross or Federated** account.

Field description for the ACM Private CA section

Field	Description
CA Operation Mode*	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • ACM • PCA
S3 Bucket*	**NOTE**: This field is displayed only when the **PCA** operation mode is selected. a. Enter the S3 bucket name. b. Click . The **ARN Advanced Settings** action pane is displayed. c. In the **ARN Advanced Settings** action pane, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming</td></tr><tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session. Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr><tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • Minimum: 900 seconds (15 minutes) • Maximum: 129,600 seconds (36 hours) Default: 3600 seconds (1 hour)</td></tr></table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr><tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr><tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: i. In the Enter Key field, enter a key for the key-value pair. ii. In the Enter Value field, enter a value for the key-value pair. iii. Click Add.</td></tr></table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>The added key-value pair is shown in the table below the fields.</td></tr>
</table>
d. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

10. Enter/Select the required details in the **EC2 Services** section.

Field description for the EC2 Services section

Field	Description
Communication mode	By default, the **SSM** communication mode is selected.
Certificate Discovery Mode	By default, the **File System Scanning** certificate discovery mode is selected.
***S3 Deployment Type**	From the dropdown list, from the following options, select the deployment type used for the S3 bucket that will be used for the EC2 integration: • **Centralized**: Select this if the S3 bucket that will be used for the EC2 integration is managed centrally across all accounts. • **Account Specific**: Select this if each account manages individual S3 buckets.
***S3 Bucket Name**	Enter the name of the S3 bucket that will be used for EC2 integration. For account specific S3 buckets, enter the bucket name **without** the account number suffix. AppViewX will automatically append the account number based on the value entered here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To configure the ARN advanced settings for the specified S3 bucket, follow the instructions given below:
a. Click .
The ARN Advanced Settings dialog box is displayed.
b. In the ARN Advanced Settings dialog box, enter the following details:
<table><tr><th>Field</th><th>Description</th></tr><tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming.</td></tr><tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr><tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
• Default: 3600 seconds (1 hour)</td></tr><tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr><tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr><tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.</td></tr></table></td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

11. To add the new device to the cloud device inventory, click **Add**.

> **Tip:** To select multiple services for a device, after you click **Add**, go back to the **Services** dropdown list and select the next service you want to enable for the device. Enter/select the rest of the details and click **Add**. Repeat this process for as many services you want to enable for the new device. The table is populated with a separate entry for each service.

- Details of the child accounts for the added master account are displayed in the inner inventory table at the bottom of the page. The details captured in the inner inventory are explained here.
- Details of the master account are listed on the **CERT+** > **Administration** > **Certificate Authority** > **<Selected CA>** page.

> **Note:** For a public Certificate Authority, only the child account details are listed on the **CERT +** > **Administration** > **Certificate Authority** > **Amazon** > **ACM CA** page. There is no inner inventory for a public certificate authority.

12. After enabling all the services for the new device, click **Save**.
    - On saving the device, through SSM, AppViewX will communicate with EC2 instances through SSM.
    - AppViewX will discover the processes from these instances and manage them in the Server device inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

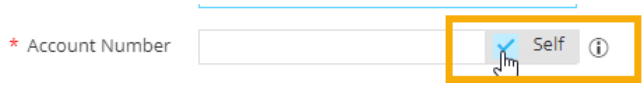
Once all the details are entered, you can add them to the Apache Linux server.

Note: Apart from the Apache and Tomcat processes vendor, the rest of the processes will be managed in the server inventory only as "Generic Linux".

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.
   The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:
- If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Onboarding a Cross Account in AppViewX for IAM Policy-based Discovery

The following instructions will guide you through the process of onboarding a standalone account in AppViewX for the supported AWS services (listed and explained here):

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	To onboard a cross account for IAM policy-based discovery: a. Select **Policy Based Discovery**. The **Policy based Discovery** dialog box is displayed. b. Enter/Select the details required to configure IAM policy-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Organization Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the services required for the CLM operations. **Tip:** To select all services, select the **Select all** check box displayed at the beginning of the list of services. **Note:** • When **ACM (Certificate Authority)** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Certificate Authority Service**to configure the ACM services. These fields are explained in the table in Step 10. • When **Amazon Private CA** is selected from the **Service** dropdown list, an additional set of fields is displayed under the section **ACM Private CA**. These fields are explained in the table in Step 11. • When the **EC2(EC2 Instance)** service is selected, an additional set of fields is displayed to configure the EC2 services. These fields are explained in the **EC2 Services** table in Step 7.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **ACM Certificate Authority Service** section.

Note: This section is displayed only when one or both **ACM** services are selected from the **Services** dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the ACM Certificate Authority Service

Field	Description
Role Setting Preference*	**Note:** This field is displayed only when both auto discovery modes (**Organization Based Discovery** and **IAM Policy Based Discovery**) are selected. From the dropdown list, select one of the following options: • **Organization Based Discovery** • **IAM Policy Based Discovery**
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle.
**: Mandatory fields*	

9. Enter/Select the required details in the **ACM Private CA** section.

Note: This section is displayed only when the **ACM (Amazon Private CA)** service is selected for a **Cross or Federated** account.

Field description for the ACM Private CA section

Field	Description
CA Operation Mode*	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • ACM • PCA
S3 Bucket*	**NOTE**: This field is displayed only when the **PCA** operation mode is selected. a. Enter the S3 bucket name. b. Click .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
The ARN Advanced Settings action pane is displayed.

c. In the ARN Advanced Settings action pane, enter the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming</td></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:

• Minimum: 900 seconds (15 minutes)

• Maximum: 129,600 seconds (36 hours)

Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.
The added key-value pair is shown in the table below the fields.</td></tr>
</table>
d. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

10. Enter/Select the required details in the **EC2 Services** section.

Field description for the EC2 Services section

Field	Description
Communication mode	By default, the **SSM** communication mode is selected.
Certificate Discovery Mode	By default, the **File System Scanning** certificate discovery mode is selected.
***S3 Deployment Type**	From the dropdown list, from the following options, select the deployment type used for the S3 bucket that will be used for the EC2 integration: • **Centralized**: Select this if the S3 bucket that will be used for the EC2 integration is managed centrally across all accounts. • **Account Specific**: Select this if each account manages individual S3 buckets.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*S3 Bucket Name</td><td>Enter the name of the S3 bucket that will be used for EC2 integration.

For account specific S3 buckets, enter the bucket name without the account number suffix. AppViewX will automatically append the account number based on the value entered here.

To configure the ARN advanced settings for the specified S3 bucket, follow the instructions given below:

a. Click .

The ARN Advanced Settings dialog box is displayed.

b. In the ARN Advanced Settings dialog box, enter the following details:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming.</td></tr>
<tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
• Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

11. To add the new device to the cloud device inventory, click **Add**.

> **Tip:** To select multiple services for a device, after you click **Add**, go back to the **Services** dropdown list and select the next service you want to enable for the device. Enter/select the rest of the details and click **Add**. Repeat this process for as many services you want to enable for the new device. The table is populated with a separate entry for each service.

- Details of the child accounts for the added master account are displayed in the inner inventory table at the bottom of the page. The details captured in the inner inventory are explained here.
- Details of the master account are listed on the **CERT+** > **Administration** > **Certificate Authority** > **<Selected CA>** page.

> **Note:** For a public Certificate Authority, only the child account details are listed on the **CERT +** > **Administration** > **Certificate Authority** > **Amazon** > **ACM CA** page. There is no inner inventory for a public certificate authority.

12. After enabling all the services for the new device, click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- On saving the device, through SSM, AppViewX will communicate with EC2 instances through SSM.
- AppViewX will discover the processes from these instances and manage them in the Server device inventory.

Once all the details are entered, you can add them to the Apache Linux server.

Note: Apart from the Apache and Tomcat processes vendor, the rest of the processes will be managed in the server inventory only as "Generic Linux".

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.

   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

> **Note:**
> - If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
> - Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.

   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

Note: This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

AWS IAM Prerequisites for Master Account

Permissions for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:GetUserPolicy",
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "iam:ListAttachedUserPolicies",
      "iam:ListAttachedGroupPolicies",
      "iam:ListUserPolicies",
      "iam:GetGroupPolicy",
      "iam:GetUser"
    ],
    "Resource": "*"
  }
 ]
}
```

Permissions for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Permissions for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": [
    "arn:aws:iam::<child account 1>:role/<Assume-role>",
    "arn:aws:iam::<child account 2>:role/< Assume-role>",
    "arn:aws:iam::<child account 3>:role/< Assume-role>"
   ]
  }
 ]
}
```

Permissions for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 ]
}
```

Permissions for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
         "Resource": "arn:aws:iam::<child-account>:role/AppViewX-S3-Bucket-Access"
      }
   ]
}
```

Permissions for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
    }
  ]
}
```

AWS IAM Prerequisites for Child Account

Permissions for Establishing a Trust Relationship in Child Accounts

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::master-account-number:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

Permissions for Discovering and Managing SSL Certificates in ACM

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Discovering and Managing SSL Certificates in CloudFront

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "acm:GetCertificate",
        "acm:ListCertificates",
        "iam:ListServerCertificates",
        "ec2:DescribeRegions",
        "cloudfront:ListDistributions",
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate",
        "acm:ListTagsForCertificate",
        "acm:RemoveTagsFromCertificate",
        "cloudfront:UpdateDistribution",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListTagsForResource",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Managing SSM Permissions for the EC2 Policy

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ec2:DescribeInstances",
  "s3:ListAllMyBuckets",
  "ssm:DescribeInstanceInformation",
  "ssm:GetDocument",
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Managing SSM Permissions for EC2 Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeDocument",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ssmmessages:OpenControlChannel",
                "ec2messages:DeleteMessage",
                "ssm:UpdateInstanceInformation",
                "ec2messages:FailMessage",
                "ssmmessages:OpenDataChannel",
                "ssm:GetDocument",
                "ssm:ListTagsForResource",
                "ec2messages:AcknowledgeMessage",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ec2messages:SendReply"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:PutObject",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::appviewx-s3/*",
                "arn:aws:s3:::appviewx-s3"
            ],
            "Effect": "Allow"
        }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  ]
}
```

Permissions for Enabling S3 Bucket Access to AppViewX

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "s3:GetObject",
  "s3:ListBucket",
  "s3:DeleteObject",
  "s3:GetBucketLocation"
         ],
         "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
         ],
      }
   ]
}
```

Permissions for Discovering and Managing SSL Certificates in ELB

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
            "elasticloadbalancing:ModifyListener",
            "ec2:DescribeInstances",
            "iam:ListServerCertificates",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "elasticloadbalancing:DescribeTags",
            "ec2:DescribeRegions",
            "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeListeners",
            "ec2:DescribeAvailabilityZones",
            "acm:GetCertificate",
            "elasticloadbalancing:DescribeTargetHealth",
            "acm:ListCertificates",
            "elasticloadbalancing:DescribeTargetGroups",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "elasticloadbalancing:AddListenerCertificates",
            "elasticloadbalancing:DescribeListenerCertificates"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Discovering and Managing Certificates in IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Discovering and Managing Private CA Certificates

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "acm:RenewCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "acm-pca:CreateCertificateAuthorityAuditReport",
 "acm-pca:DescribeCertificateAuthorityAuditReport,
 "acm-pca:GetCertificate",
 "acm-pca:ListCertificateAuthorities",
 "acm-pca:IssueCertificate",
 "acm-pca:RevokeCertificate",
 "s3:GetBucketLocation",
 "s3:GetObject"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        ],
        "Resource": "*"
      }
    ]
}
```

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

- Create an IAM user in your AWS account
- Create access keys for the root user
- Create IAM policies using the JSON editor
- Accessing member accounts
- Using IAM roles for Amazon EC2 instances
- Define custom IAM permissions for customer managed policies
- Creating, configuring, and working with Amazon S3 general purpose buckets

What's Next?

After you have successfully onboarded a cross account in AppViewX, the next step is to discover existing certificates for the onboarded account and/or enroll new certificates.

AWS Standalone Account Onboarding via Cross Account

The process of onboarding a cross or federated account access involves the following steps:

Step 1: Creating an S3 bucket using the Cloudformation template

1. Login to the AWS account and go to the **CloudFormation service** section.
2. From the navigation pane on the left, select **Stacks**.
3. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.
4. In the **Prerequisite - Prepare Template** section, select the **Template is ready** option.
5. In the **Specify template** section:
   a. For **Template source**, select **Upload a template file**.
   b. To **Upload a template file**, click **Choose file**.
   c. Navigate to the **CloudFormationTemplates/WithoutCondition** folder.
   d. Select the **S3Bucket.yaml** file and click **Open**.
6. Click **Next**.

   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Enter a **Stack name**. For the purpose of this guide, **Stack name** = **avxdemo-S3**.
8. In the **Parameters** section, enter the following details:

    a. **AccountId**: From the top-right corner of the screen, click your username and copy the account ID displayed.

    b. **BucketName**: Enter a name for the S3 bucket that will be created in the backend. Recommended format to name the S3 bucket: **avxdemo-<account ID>**.

    c. **OrganizationID**:
        i. From the top-right corner of the screen, click your username.
        ii. From the menu displayed, right click **Organization** to open it in a new tab.

        The **Dashboard** is displayed.

        iii. From the **Dashboard**, copy the organization ID and paste it into the **OrganizationID** field.

        > **Note:** The organization ID is a mandatory entry for the CloudFormation template.

    d. **RoleName**: Enter a name for the S3 bucket role. For the purpose of this guide, the S3 bucket role will be called **avxdemos3bucketrole**.

    The details entered on the **Specify stack details** page will be used to create a bucket policy for the S3 bucket created for the AWS account. This bucket policy can be customized later based on customer preferences for how they want to secure their infrastructure.

9. Click **Next**.
    The **Configure stack options** page (step 3 of the stack creation process) is displayed.
10. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
11. Click **Next**.
    The **Review <stack name>** page (step 4 of the stack creation process) is displayed
12. On the **Review <stack name>** page, scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.
13. Click **Create stack**.

    The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

    - **Stack info**
    - **Events**
    - **Resources**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Outputs**
- **Parameters**
- **Templates**
- **Change sets**

When the stack creation process is complete, **Status** (under the **Events** tab) will be updated to **CREATE_COMPLETE**. This means that, in the backend, an S3 bucket as well as the roles required to provision the bucket have been created. The bucket policy for the S3 bucket has also been updated accordingly.

14. Go to the **Parameters** tab and note the bucket name to use it in the CloudFormation template for the master account.

What to do next: Create a child account using the CloudFormation template.

Step 2: Creating a child account using the CloudFormation template

1. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.

2. From the navigation pane on the left, click **Step 2 Specify stack details**.
   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.
3. Enter a **Stack name**. For the purpose of this guide, **Stack name** = **avxdemoc1**.
4. In the **Parameters** section, enter the following details:
   a. **MasterAccountNumber**: From the top-right corner of the screen, click your username and copy the account ID displayed. Paste it in the **MasterAccountNumber** field.
   b. **S3BucketName**: Enter the S3 bucket name copied from the **Parameters** tab of the **avxdemo-S3** stack.
5. Click **Next**.

   The **Configure stack options** page (step 3 of the stack creation process) is displayed.

6. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
7. Click **Next**.

   The **Review <stack name>** page (step 4 of the stack creation process) is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. Scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.
9. Click **Create stack**.

   The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

   - **Stack info**
   - **Events**
   - **Resources**
   - **Outputs**
   - **Parameters**
   - **Templates**
   - **Change sets**

   When the stack creation process is complete, **Status** (under the **Events** tab) will be updated to **CREATE_COMPLETE**.
10. Navigate to the **Resources** tab for the **avxdemoc1** stack.
    You will see that a policy called **AppViewXCLM** has been created. This policy will have all the permissions and prerequisites required for AppViewX to discover all the ACM, ELB, and EC2 instances.
11. Navigate to the **Outputs** tab for the **avxdemoc1** stack.
    Note down the **ChildRoleARN** to use it in the CloudFormation template for the master account.

What to do next: Create a master account using the CloudFormation template.

Step 3: Creating a master account using the CloudFormation template

1. Go to the **CloudFormation service** section.
2. From the navigation pane on the left, select **Stacks**.
3. From the top-right corner of the **CloudFormation** > **Stacks** screen, click **Create stack** > **With new resources (standard)**.

   The **Create stack** page is updated to display the fields for **Step 1 Specify template** of the stack creation process.
4. In the **Prerequisite - Prepare Template** section, select the **Template is ready** option.
5. In the **Specify template** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. For **Template source**, select **Upload a template file**.
b. To **Upload a template file**, click **Choose file**.
c. Navigate to the **CloudFormationTemplates/WithoutCondition** folder.
d. Select the **master_account.yaml** file and click **Open**.

6. Click **Next**.

   The **Specify Stack Details** page (step 2 of the stack creation process) is displayed.

7. Enter a **Stack name**. For the purpose of this guide, **Stack name** = **avxdemom1**.
8. In the **Parameters** section, enter the following details:

   a. For **ApplyAssumeRoleForAll**, from the dropdown list, select **False**.

   b. From the **Outputs** tab of the **avxdemoc1** CloudFormation template for the child account, copy the **ChildRoleARN** and paste it in the following fields:
   • **ChildRoleARN**
   • **OrganizationRoleARN**

   c. From the **Outputs** tab of the **avxdemo-S3** CloudFormation template, copy the **S3BucketAssumeRole** and paste it in the following fields:
   • **S3BucketRoleARN**
   • **SQSRoleARN**

   d. In the **UserName** field, enter a username for the IAM account. For the purpose of this guide, the username will be set to **avxdemo-user**.

9. Click **Next**.
   The **Configure stack options** page (step 3 of the stack creation process) is displayed.
10. Scroll down to the **Stack failure options** section and select **Preserve successfully provisioned resources**.
11. Click **Next**.
    The **Review <stack name>** page (step 4 of the stack creation process) is displayed
12. Scroll down to **Capabilities** and select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** checkbox.
13. Click **Create stack**.

    The **<stack name**> page is displayed. This page lists the existing stacks on the left and the following details for each stack on the right:

    • **Stack info**
    • **Events**
    • **Resources**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Outputs**
- **Parameters**
- **Templates**
- **Change sets**

14. From the **Outputs** tab of the stack, note the access key and the secret key information to use in AppViewX.

What to do next: Map the EC2 roles to the customer's EC2 instances.

Step 4: Mapping EC2 roles to a customer's EC2 instances

The EC2 role created using the CloudFormation template with the naming convention **<Stack_Name>-Ec2RoleForSSM** must be mapped to the EC2 instances. This mapping is required for enabling SSM communication between the instances and AppViewX and for enabling access to the S3 buckets to store the SSM run command response.

What to do next: Test device onboarding the AppViewX environment.

Step 5: Testing Onboarding in the AppViewX Environment

1. Login to AppViewX.
2. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
3. From the **Device :: ADC** page, select **Cloud**.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **AWS**.
5. Enter/select the **Basic information**.

Field description for the Basic information section

Field	Description
Account type*	From the dropdown list, select **Cross or Federated**.
Account name*	Enter the account name, **avxdemo**.
Account number*	Enter the AWS account number.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account Description	Enter a description of the device to be added.
Proxy required	To use a proxy server for the communication, select this checkbox.
Default Region*	From the dropdown list, select a default region for the API communication.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
**: Mandatory fields*	

6. Enter the **Credentials**-related details:

Field descriptions for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: To manually enter the access and secret key for the customer's AWS account) • **Credential List - CyberArk**: To automatically retrieve the customer's AWS key details from CyberArk)
Access key*	Copy the **AccessKey** from the **Outputs** tab of the **avxdemom1** template.
Secret key*	Copy the **Secret Access Key** from the **Outputs** tab of the **avxdemom1** template.
**: Mandatory fields*	

7. Enter the details required to **Discover resources**.

Field descriptions for the Discover resources section

Field	Description
Auto Discover Resources*	By default, the **Auto Discover Resources** toggle key is set to **ON** and is non-editable. Enabling this feature allows discovering all the cross or federated/child accounts for the provided master account details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Advanced Settings*	By default, the **Advanced Settings** toggle key is set to **ON** and is non-editable. This feature allows customizing the auto discovery process.
AutoSync	To enable automatic synchronization, enable this toggle.
Auto Discovery Mode*	Select the **IAM Policy**.
Services*	Select the ACM, ELB, and EC2 services (and their subservices, as required).
Service region*	For the purpose of this solution guide, click **Fetch Region** and select the regions US East (N. Virginia) and US West (N. California).
Route53 Zone Auto Approval*	To support DNS validation as an automatic process, turn on the **Route53 Zone Auto Approval** toggle.
Cert sync	Select one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • Minimum: 900 seconds (15 minutes) • Maximum: 129,600 seconds (36 hours) • Default: 3600 seconds (1 hour)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session name*	**Role Session name** is an identifier for the assumed role session. Use the **Role Session name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons. By default, the **Role Session name** is set to **appviewx**.
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account. For the purpose of this guide, external ID is undefined.
Source Identity	The source identity is specified by the principle that is calling the **AssumeRole** operation. For the purpose of this guide, source identity is undefined.
Session Tags	Enter the key-value attribute pairs required when assuming an IAM role or federating a user in the AWS STS.
**: Mandatory fields*	

8. In the **EC2 Services** section, copy the **S3Bucket Name** from the **Resources** tab of the **avxdemo-S3** template.
9. In the **S3 Bucket Name** field, click .
   The **ARN Advanced Settings** pop-up window is displayed.
10. Copy the **Role ARN** from the **Outputs** tab of the **avxdemo-S3** template and paste it in the **Role ARN** field.
11. Click **Apply**.
12. Click **Save**.

    The discovered account will be displayed in the grid on the **Device :: Cloud** page.

> **Note:** The discovered account will be added one more time as a child account since the use case uses federated access. This behaviour will be altered in the future releases to avoid dual listing of discovered AWS accounts.

Azure

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Important: After migrating to AppViewX v2022.1.0 and beyond, from any of the previous versions, ensure that you have entered the data centre details for each existing Azure account. For instructions to do this, follow steps 1-5 listed here.

This step is not required for migration to v2022.1.0 to any of the later versions.

Important: At the time of migrating to AppViewX v2023.1.0 FP2 and beyond, manually trigger a config fetch for all the Azure accounts already created.

This will ensure that all functionality enhancements are applied correctly.

This documentation highlights the benefits and implementation of integrating supported Azure services with AppViewX to enable comprehensive certificate lifecycle management across Azure environments. The complete list of supported services, along with an overview of each, is provided in the section Azure Subscriptions and Services Supported by AppViewX.

- Azure Subscriptions and Services Supported by AppViewX
- Permissions Required for Onboarding Azure
- Onboarding Microsoft Azure Settings in AppViewX

Azure Subscriptions and Services Supported by AppViewX

Azure Subscriptions

Azure subscriptions are logical containers for providing and managing tenant access to Azure resources and services.

AppViewX supports two Azure subscription types: **single** and **multi**. The **difference between single and multiple subscriptions in Azure implementations** lies in how resources are organized, managed, and accessed.

- **Single Subscription**: Resources are hosted and managed in a single subscription.
- **Multi Subscription**: Resources are divided across subscriptions, allowing for isolated management and granular access control to resources.

Azure Services

AppViewX supports the following Azure services:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Key Vault**

  The Azure Key Vault is a key management solution from Microsoft that offers the following features:

  - Secrets Management: The key vault can be used for securely storing and managing access to tokens, passwords, API keys, and other secrets.
  - Key Management: The key vault simplifies the creation and management of encryption keys used for data encryption.
  - Certificate Management: Azure key vault simplifies the certificate lifecycle management of TLS/SSL certificates

- **Application Gateway**

  The Azure Application Gateway is a web traffic load balancer that helps to optimize and secure web applications traffic. The application gateway operates at the application layer of the OSI model and makes routing decisions based on attributes of an HTTP request, for example the URI path or the host headers.

- **Virtual Machines**

  Azure Virtual Machines (VMs) are scalable and flexible computing resources provided by Microsoft Azure. They enable users to run virtualized Windows or Linux servers in the cloud. Azure VMs allow you to quickly deploy and manage virtualized infrastructure to support various applications, workloads, and services.

  Important: Please note the following **limitations** for Azure virtual machines:
  - Currently, only the Linux-based VMs (and not Windows-based VMs) are discovered.
  - The discovered/onboarded VMs are listed in the server device inventory.
    You are required to manually update the VM credentials in the server inventory to proceed with certificate lifecycle management for the VM.

    To access the server inventory, Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management** and open the **Server** tab.

- **App Service**

  App Services is a fully managed platform for building, deploying, and scaling web apps, mobile app backends, and RESTful APIs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- For all app services in an Azure subscription, AppViewX can discover and manage public and private certificates that have been referenced via a key vault; a single key vault can be used for all app services.
- For app services certificates, can be pushed directly to app services or it can be pushed to key vault and referenced from app services. However, currently, there is no support for certificates directly onboarded to the app services.

- **Enterprise Application**

  The Enterprise Application service in Azure is a key component of Azure Active Directory (Azure AD) used to manage access to applications in a secure and streamlined manner. It allows organizations to integrate both Microsoft and third-party applications with Azure AD for identity and access management.

  Its key features include:
  - Single Sign-On access to multiple applications
  - Secure application management by enabling access policy configuration, access control based on users and groups, and multi-factor authentication.
  - Role-based Access Control (RBAC)
  - Conditional access to applications, including MFA for sensitive applications
  - Monitoring and reporting for application usage, sign-in activities, security risks, and anomalies
  - Identity management by integration with Azure AD
- **API Management**

  The API Management service helps create, manage, secure, and monitor APIs. It provides a centralized platform for API publishers to control their APIs, while enabling developers to consume them in a secure and efficient manner.

  Its key features include:
  - API Gateway that routes all incoming requests to the appropriate backend services
  - Developer Portal that can be customized to help developers discover and access APIs
  - API versioning with revision tracking
  - Authentication and authorization mechanisms for secure access control to APIs
  - Rate limiting and throttling to protect backend services from excessive or abusive traffic
  - Analytics and monitoring
  - Policy Engine to implement additional logic at the API Gateway
- **App Registration**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The App Registration service enbales identity and access management, API security, and integration capabilities. It is used for registering and configuring applications for interactions with Azure services.

App Registration service is essential when you want to allow your application to authenticate users or access resources such as APIs in a secure way.

Its key features include:

- Application Identity Management
- Authentication Support
- Access permissions and scope definition for APIs
- Multi-Tenant and Single-Tenant support
- Enterprise Application Integration
- Roles and Role-Based Access Control
- Token Issuance and Validation for Authentication and Authorization
- Auditing and Monitoring
- Conditional Access and Multi-Factor Authentication

- **Front Door**

Azure Front Door is a modern, high-performance, and secure cloud Content Delivery Network (CDN) that serves as the global entry point for your applications. It optimizes traffic by routing users to the nearest edge location for faster, more reliable access, while built-in caching, acceleration, and a Web Application Firewall (WAF) provide enhanced performance and protection—making it ideal for global websites and SaaS applications.

Permissions Required for Onboarding Azure

Note: For Azure, a custom role has to be created and assigned to the service principal.

Important: In the following sample permissions, the value for **subscriptions** is a placeholder. You are required to replace it with your actual subscription ID.

Permissions for Key Vault

Certificates

```
{
  "properties": {
    "roleName": "AppViewX_KeyVault_Role",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "description": "",
  "assignableScopes": [
    "/subscriptions/000-000-000-0000-000"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.KeyVault/vaults/read"
      ],
      "notActions": [],
      "dataActions": [
        "Microsoft.KeyVault/vaults/certificates/import/action",
        "Microsoft.KeyVault/vaults/certificates/create/action",
        "Microsoft.KeyVault/vaults/certificates/update/action",
        "Microsoft.KeyVault/vaults/certificates/read"
      ],
      "notDataActions": []
    }
  ]
 }
}
```

Secrets

```
{
 "properties": {
  "roleName": "AppViewX_KeyVault_Secret_Role",
  "description": "",
  "assignableScopes": [
    "/subscriptions/000-000-000-0000-000"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.KeyVault/vaults/secrets/read"
      ],
      "notActions": [],
      "dataActions": [
        "Microsoft.KeyVault/vaults/secrets/setSecret/action",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "Microsoft.KeyVault/vaults/secrets/getSecret/action",
        "Microsoft.KeyVault/vaults/secrets/readMetadata/action"
      ],
      "notDataActions": []
    }
  ]
 }
}
```

Permissions for Application Gateway

> **Important:** Use the permission `Microsoft.ManagedIdentity/userAssignedIdentities/assign/action` only if the application gateway has to be integrated with the key vault.

```
{
  "properties": {
    "roleName": "AppViewX_AppGW_Permission",
    "description": "",
    "assignableScopes": [
      "/subscriptions/000-000-000-0000-000"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Network/applicationGateways/write",
          "Microsoft.Network/applicationGateways/read",
          "Microsoft.Network/applicationGatewayAvailableSslOptions/predefinedPolicies/read",
          "Microsoft.Network/applicationGatewayAvailableSslOptions/read",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  }
}
```

Permissions for Virtual Machine

```
{
 "properties": {
  "roleName": "AppViewX_VirtualMachine_Role",
  "description": "",
  "assignableScopes": [
   "/subscriptions/000-000-000-0000-000"
  ],
  "permissions": [
   {
    "actions": [
     "Microsoft.Compute/virtualMachines/read",
     "Microsoft.Network/networkInterfaces/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
   }
  ]
 }
}
```

Permissions for App Service

> **Important:** Use the permission `Microsoft.ManagedIdentity/userAssignedIdentities/assign/action` only the application gateway needs integration with the key vault.

```
{
  "properties": {
    "roleName": "AppViewX_App_Service_Permission",
    "description": "",
    "assignableScopes": [
      "/subscriptions/000-000-000-0000-000"
    ],
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "permissions": [
      {
        "actions": [
            "Microsoft.Web/sites/Read",
          "Microsoft.Web/sites/Write",
          "microsoft.web/sites/publiccertificates/read",
            "microsoft.web/sites/publiccertificates/write",
            "Microsoft.Web/sites/restart/Action",
            "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Permissions for Enterprise Application

The user should have access to the following Graph APIs:

- **Application.Read.All**
- **Application.ReadWrite.All**

Permissions for API Management

> **Important:** Use the permission `Microsoft.ManagedIdentity/userAssignedIdentities/assign/action` only the application gateway needs integration with the key vault.

```
{
  "properties": {
    "roleName": "AppViewX_APIMngmnt_Permission",
    "description": "",
    "assignableScopes": [
      "/subscriptions/000-000-000-0000-000"
    ],
    "permissions": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        {
            "actions": [
                "Microsoft.ApiManagement/service/certificates/read",
                "Microsoft.ApiManagement/service/certificates/write",
                "Microsoft.ApiManagement/service/certificates/delete",
                "Microsoft.ApiManagement/service/certificates/refreshSecret/action"
                "Microsoft.ApiManagement/service/read",
                Microsoft.ManagedIdentity/userAssignedIdentities/assign/action
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
    ]
  }
}
```

Permissions for App Registration

The user should have access to the following Graph APIs:

- **Application.Read.All**
- **Application.ReadWrite.All**

Permissions for Front Door

```
{
   "properties": {
      "roleName": "AppViewX_FrontDoor_Permission",
      "description": "",
      "assignableScopes": [
         "/subscriptions/000-000-000-0000-000"
      ],
      "permissions": [
         {
            "actions": [
               "Microsoft.Resources/subscriptions/resources/read",
               "Microsoft.Cdn/profiles/customDomains/read",
               "Microsoft.Cdn/profiles/secrets/read",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                "Microsoft.Cdn/profiles/customDomains/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
    ]
  }
}
```

Onboarding Microsoft Azure Settings in AppViewX

Prerequisites for Onboarding Microsoft Azure Settings in AppViewX

- Depending on the service(s) selected for the Azure configuration, ensure that the corresponding service instance is created in your Microsoft Azure account.

  For links to the complete Microsoft Azure documentation for the supported services, refer the References section.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Onboarding Microsoft Azure Settings in AppViewX

The following instructions will guide you through the process of onboarding a Microsoft Azure account in AppViewX for the supported Microsoft Azure services (listed and explained here):

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity**: [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. To validate the credential details entered above, click **Validate Credential**.

> **Note:** The option to **Validate Credential** is displayed only for a multi subscription account type.

Access to the **Discover Resources** section is enabled only after the credentials have been validated.

8. Enter/Select the details needed to **Discover Resources**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Discover Resources section

Field	Description
***Services**	From the following options in the dropdown list, select the service(s) that will be mapped to this setting (for an overview of each supported service, see Azure Subscriptions and Services Supported by AppViewX): • Api Management • App Registration **Note:** Currently, this service is not supported for multi subscription accounts. • App Service • Application Gateway • Enterprise Application [For instructions on managing Enterprise Application certificates, click here.] **Note:** Currently, this service is not supported for multi subscription accounts. • Front Door • Key Vault • Virtual Machines Starting v2024.1.0.0, Linux-based as well as Windows-based VMs can be discovered. For instructions on managing the Linux-based/Windows-based server devices onboarded as VMs, click here.
***Subscription ID**	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. This is an **optional** field for the following Azure servcies: • App Registration • Enterprise Application

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the unique identified (GUID) of your Azure subscription.
Subscription Onboarding State	Subscription onboarding refers to integrating an Azure subscription with AppViewX. You can choose to onboard all subscriptions at once or onboard only selected ones. From the following options, select a state for onboarding subscriptions discovered from the Azure organization: • **Managed**: Enables subscription onboarding, allowing Azure cloud resource and certificate discovery instantly • **Unmanaged**: Disables subscription onboarding, preventing resource and certificate discovery for these projects. After you have fetched all subscriptions belonging to these projects, you can select individual subscriptions for onboarding, as explained here.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

9. For a multi subscription account, after specifying the details for resource discovery, click **Fetch Subscriptions**.
   a. From the subscriptions table, select the checkbox corresponding to the subscription(s) you want to manage.
   b. From the **Actions** dropdown menu, select **Manage**.
10. In the **Additional attributes** section for the selected services, select the user permission for **Cert sync** from the following options:

    a. For the selected services, select the user permission for **Cert sync** from the following options:
    - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
    - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
    - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

b. For **Enterpise Application**, enter/select the following additional details:

Field descriptions for the additional Enterprise Application attributes

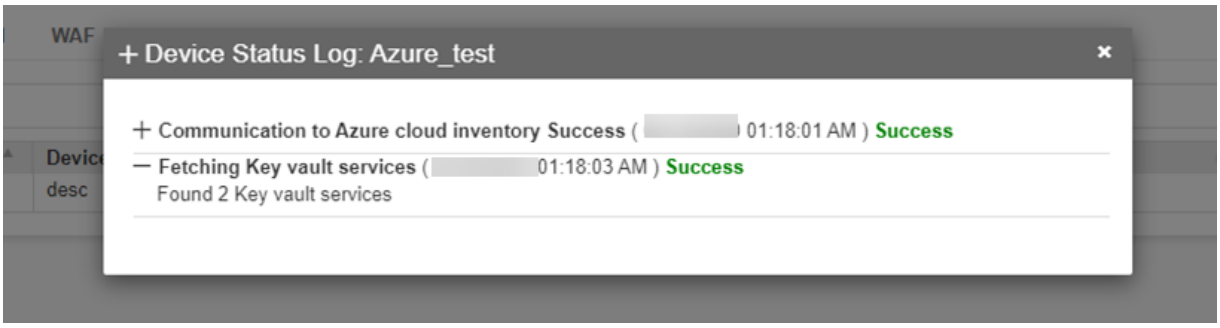
Field	Description
Discover Inactive Certificates	The Enterprise Application service has an active certificate associated with it, which is the default certificate used for securing communication, authentication, and encryption. The rest of the certificates associated with this service are categorized as inactive certificates. To enable discovery of inactive certificates along with the active certificate associated with the selected service(s), enable the **Discover Inacrive Certificates** toggle button.
Notify For	You can choose to receive email notifications every time: • a certificate is pushed to the Enterprise Application service • a certificate is made active certificate while being pushed to the Enterprise Application service To receive email notifications: i. Enable the **Notify For** toggle button. ii. To receive notifications when a certificate is pushed, select **Push**. To receive notifications when a certificate is made active certificate while being pushed, select **Make Certificate Active**.
***Email Alert Template**	**Note:** This field is displayed only when **Notify For** is enabled. From the list of predefined email templates in the dropdown list, select the email template that will be used to send the alert. **Note:** To view the predefined templates, go to **Platform** > **System Administration** > **Themes & Personalization** > **Email attachment customization**. The predefined templates are listed in the **Email Template** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Email Subject**	**Note:** This field is displayed only when **Notify For** is enabled. Enter a custom email subject for the notification email.
Attach Certificates to Email Body	**Note:** This field is displayed only when **Notify For** is enabled. If you need the relevant certificate(s) attached to the notification email, from the following options, select the format in which the certificate will be shared: • **Include as Content** The email body includes the contents of the certificate. If the certificate being pushed is an inactive certificate, the email will also include instructions for manually making it the active certificate. • **Include as Downloadable Link** (to include The email body includes a link for downloading the certificate. Clicking the link will redirect you to the holistic view of the certificate, from where you can download the certificate.
**: Mandatory fields*	

11. Click **Save**.
12. Return to the **Device :: Cloud** page.
13. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



14. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Managing Enterprise Application Certificates

Starting v2024.0.1.0, self-signed certificates discovered from the Enterprise Application service can be:

- Renewed
- Made active

Renewing an Enterprise Application Self-Signed Certificate

To renew an Enterprise Application Self-Signed Certificate,

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the Enterprise Application Self-Signed Certificate that you want to renew.
   The holistic view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Renew**.
4. In the **Renew** dialog box:
   a. Enter the new **Validity** for the renewed certificate.
   b. To make the certificate active, select the **Make Certificate Active** checkbox.
5. Click **Renew**.
   A request ID, which is the work order ID, is generated automatically, and work order status is displayed adjacent to the certificate in the holistic view. If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
6. In the holistic view, click **Approve** to proceed.
   The **Approve** dialog box is displayed.
7. Enter your comments in the text field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

8. Click **Yes**.
   Once the approval process is complete, the **Implement** option is displayed in the holistic view.
9. Click **Implement**.
   The **Implement** dialog box is displayed.
10. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
11. Click **Yes**.
    The renewal process is triggered. After renewal is completed:
    • Workflow status is updated to **Completed**.
    • A notification email is sent.
12. To see if the certificate has been made active (if you selected the checkbox), hover over the application connector for the certificate.
    If the certificate is active, the **Is Active** field in the tooltip text is set to **Yes**.

Making an Enterprise Application Self-Signed Certificate Active

There are two ways in which you can make an Enterprise Application self-signed certificate active.

- By selecting the **Make Certificate Active** checkbox from the **Renew** dialog box for the self-signed certificate

  The instructions for this are given here.

- By selecting the **Make Certificate Active** option from the **More** menu in the holistic view

  The instructions for this are given below.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the Enterprise Application Self-Signed Certificate that you want to make active.
   The holistic view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Make Certificate Active**.
4. To see if the certificate has been made active, hover over the application connector for the certificate.
   If the certificate is active, the **Is Active** field in the tooltip text is set to **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Managing Server Devices Onboarded as Azure Virtual Machines

The discovered/onboarded VMs are listed in the server device inventory.

To access the server device inventory, Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management** and open the **Server** tab.

Once the server device is onboarded, you are required to manually update the VM credentials in the server inventory to proceed with certificate lifecycle management for the VM.

To do this:

1. Go to the server device inventory.
2. On the **Device :: Server** page, click the device **Name** to modify the device details.
   You will be redirected to the **Device details** page.
3. In the **Credentials** section, update the device credentials.
   For field descriptions and other details, refer from the following links:
   - Configuring Linux Server
   - Configuring Microsoft Server

References

- Create an Azure Key Vault using the Azure Portal.
- Create an Azure Application Gateway using the Azure Portal.
- Create a Linux Virtual Machine using the Azure Portal.
- Create a Windows Virtual Machine using the Azure Portal.
- Getting Started with the Azure App Service.
- Add an Enterprise Application.
- Create a new Azure API Management Instance by using the Azure Portal.
- Create an Azure Front Door Profile using the Azure Portal.
- Configure managed identities on Azure virtual machines.

What's Next?

After you have successfully onboarded a Microsoft Azure account in AppViewX, the next step is to discover existing certificates for the onboarded account and/or enroll new certificates.

Google Cloud Platform (GCP)

Google Cloud Platform (GCP) is a suite of computing services provided by Google, that can be integrated with an organization’s multicloud setup to meet specific business requirements.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Using GCP in a multicloud setup offers the following advantages:

- Diversity of services (especially in the areas of big data, machine learning, and data analytics) to enhance the overall capabilities of your organization's infrastructure
- Access to advanced analytics and process automation tools
- Support for data analytics and big data capabilities
- Global network infrastructure known for its speed and reliability
- Security expertise
- Data storage and management capabilities

- GCP Services Supported by AppViewX
- Onboarding a Single GCP Project
- Onboarding GCP Projects within an Organization
- Project-level/Inner Inventory
- Limitations

GCP Services Supported by AppViewX

AppViewX supports the following GCP services:

- **Certificate Manager**

  Certificate Manager is a managed GCP service that automates the process of obtaining, issuing, and renewing certificates, and then seamlessly integrating to provision your certificates for the load balancer.

- **Load Balancer**

  GCP comes with a set of load balancers that distribute incoming network traffic evenly across multiple instances or services. Load balancers ensure that your multicloud setup conforms to the requirements of high availability, fault tolerance, and scalability.

  Types of load balancers in GCP:
  - Google Cloud Load Balancer
  - Network Load Balancer
  - SSL Proxy Load Balancer
  - TCP Proxy Load Balancer
  - UDP Load Balancer
  - Internal TCP/UDP Load Balancer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Classic Certificates**

  Classic certificates is a GCP service that lets you create and manage Google-managed SSL certificates.

Onboarding a Single GCP Project

Prerequisites for Onboarding a Single GCP Project

To onboard a single GCP project in AppViewX, you are first required to create and associate roles with the project to be onboarded. For references to the GCP documentation for instructions, click **here**.

Onboarding a Single GCP Project in AppViewX

1. In the AppViewX UI, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
   The **Device** :: **ADC** page is displayed.
2. On the **Device** :: **Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
3. Under **Device details**, from the list of **Vendors**, select **GCP**.
4. Enter/Select the **Basic Information** for onboarding a single GCP project.

Field description for the basic information

Field	Description
***Onboarding Method**	From the dropdown list, select **Onboard a Single GCP Project**.
***Account Name**	Enter your unique GCP account name. **Note:** • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and the period (**.**) characters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account Description	Enter a description of the GCP account to be added.
Proxy Required	To use a proxy server for this communication, select this checkbox.
***Data Center**	From the dropdown list, select the data center through which communication with the certificate authority will be established.

5. Enter/Select the **Project & Credential Details**.

Field descriptions for the project and credential details

Field	Description
Service Account Key	To access the GCP services using AppViewX, the credentials are supplied either in a JSON or in the form of a certificate file. After you have created the GCP service account, you can download the JSON file or the certificate file with the credential details. Depending on the artifact download, from the **Service Account Key** field, select the **JSON File** or the **Certificate Upload** option.
***Upload JSON**	**Note:** This field is displayed only when **Service Account Key** = **JSON File**. Click **Upload** and navigate to the location of the JSON file.
***Certificate and Key**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Click **Upload** and navigate to the location of the certificate file.
***Email**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your email ID registered with GCP.
***Project Id**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your GCP project ID.
Validate Credential	To validate the credentials uploaded using JSON/ certificate file, click validate credential.

6. Enter/Select the details required to **Discover Resources**.

Note: The fields in this section are enabled only after the credentials entered in the **Project & Credential Details** section have been validated.

Field descriptions for discovering resources

Field	Description
***Service Type**	From the dropdown list, select the services required for CLM operations.
Cert Sync	Select from one of the following options: • **Managed**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Monitored**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with your GCP account but certificate discovery will be disabled.
Auto Sync	To enable (default)/disable automatic synchronization, use the **Auto Sync** key. Currently the GCP implementation in AppViewX only supports schedule-based synchronization.
Schedule Based Discovery	**Note:** This field is displayed when **Auto Sync** is enabled. To schedule a discovery, set the frequency using the two dropdown lists for this field. For example, to set the frequency to 10 days: a. From the first dropdown list, select **10**. b. From the second dropdown list, select **Days**.

7. Click **Save**.
   Details of the added GCP account are displayed in the outer inventory (explained here).

References

- Get Started with Google Cloud

Onboarding GCP Projects within an Organization

Prererequisites for Onboarding GCP Projects within an Organization

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To onboard GCP projects within an organization in AppViewX, at the organizational level, you are first required to create and associate roles with the projects to be onboarded. For references to the GCP documentation for instructions, click **here**.

Onboarding GCP Projects within an Organization in AppViewX

1. In the AppViewX UI, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.
   The **Device** :: **ADC** page is displayed.
2. On the **Device** :: **Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
3. Under **Device details**, from the list of **Vendors**, select **GCP**.
4. Enter/Select the **Basic Information** for onboarding a single GCP project.

Field description for the basic information

Field	Description
***Onboarding Method**	From the dropdown list, select **Onboard GCP Projects within Organization**.
***Account Name**	Enter your unique GCP account name. **Note:** • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and the period (**.**) characters.
Account Description	Enter a description of the GCP account to be added.
Proxy Required	To use a proxy server for this communication, select this checkbox.
***Data Center**	From the dropdown list, select the data center through which communication with the certificate authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Enter/Select the **Project & Credential Details**.

Field descriptions for the project and credential details

Field	Description
***Organization ID**	To discover and onboard the GCP projects within the organization, enter your unique GCP organization resource ID.
Service Account Key	To access the GCP services using AppViewX, the credentials are supplied either in a JSON or in the form of a certificate file. After you have created the GCP service account, you can download the JSON file or the certificate file with the credential details. Depending on the artifact download, from the **Service Account Key** field, select the **JSON File** or the **Certificate Upload** option.
***Upload JSON**	**Note:** This field is displayed only when **Service Account Key** = **JSON File**. Click **Upload** and navigate to the location of the JSON file.
***Certificate and Key**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Click **Upload** and navigate to the location of the certificate file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Email**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your email ID registered with GCP.
***Project Id**	**Note:** This field is displayed only when **Service Account Key** = **Certificate Upload**. Enter your GCP project ID.
Validate Credential	To validate the credentials uploaded using JSON/ certificate file, click validate credential.

6. Enter/Select the details required to **Discover Resources**.

Note: The fields in this section are enabled only after the credentials entered in the **Project & Credential Details** section have been validated.

Field descriptions for discovering resources

Field	Description
***Project Onboarding State**	From the following values, select the state for onboarding the projects discovered from the GCP organization: • **Managed**: Enables project onboarding and allows instant GCP cloud resource and certificate discovery • **Unmanaged**: Disables project onboarding, preventing resource and certificate discovery for these projects.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Service Type**	From the dropdown list, select the services required for CLM operations.
Cert Sync	Select from one of the following options: • **Managed**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with your GCP account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with your GCP account but certificate discovery will be disabled.
Auto Sync	To enable (default)/disable automatic synchronization, use the **Auto Sync** key. Currently the GCP implementation in AppViewX only supports schedule-based synchronization.
Schedule Based Discovery	**Note:** This field is displayed when **Auto Sync** is enabled. To schedule a discovery, set the frequency using the two dropdown lists for this field. For example, to set the frequency to 10 days: a. From the first dropdown list, select **10**. b. From the second dropdown list, select **Days**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Click **Save**.
   Details of the added GCP account are displayed in the outer inventory (explained here).

References

- Get Started with Google Cloud

Project-level/Inner Inventory

Field	Description
Account Name	Name of the account to which the cloud device belongs
Project ID	GCP project ID
Project Number	GCP project number
Service Type	GCP service selected for CLM operations
Service Status	**Success** or **Failure**, depending on whether the account has permission to accessthe service
Resource Discovery Status	**Note:** Resource discovery status is not applicable for organizations. For organizations, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered project using the following values: • **Not started**: Resource discovery by AppViewX is yet to begin **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery by AppViewX in the customer's GCP environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's GCP environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX in GCP. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • for ACM and ELB resources • for all existing devices and projects as part of data migration
State	Outcome of the device addition (**Success**, **Failed**)

Limitations

- Pushing certificates to the Certificate Manager and binding to the Classic Loadbalancers in the standard tier is currently not supported.

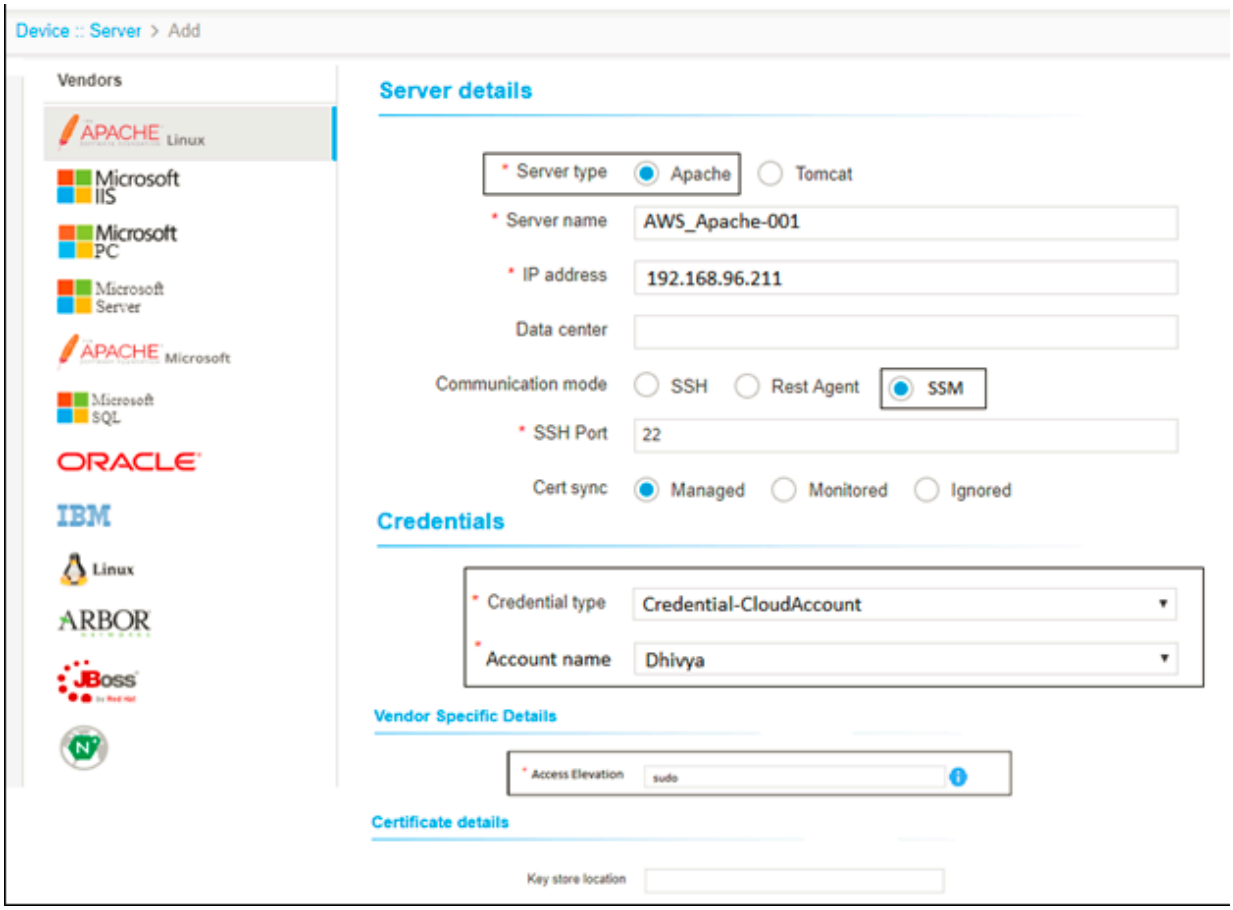
Apache SSM integration specification

Device Addition

- **Apache (Linux)** serversdiscovered from Amazon EC2 instances should be added under the Server tab in AppViewX.
- All the mandatory fields should be pre-fill in the Apache (Linux) device addition page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The server name should be appended with AWS as shown below.
- By default, the communication mode should be selected as **SSM.**
- Credential provided in cloud inventory should be used in server inventory as well.
- By default, access elevation should be selected as **Sudo.**



Credential management

- Credential Type is a mandatory field.
- When a device is added from a could account, **Credential-Cloud Account must** be displayed corresponding to the credential type label. And the cloud account name should be displayed in a dropdown corresponding to the Account name label.
- While modifying the mandatory details in the Apache form, the user should be able to select a different cloud account credential that is added to the cloud inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Similarly, while modifying the mandatory details in the Apache form, the user should be able to provide credentials manually in the Apache device addition form.

> **Note:** Once the Apache instance is identified and successfully added, the user should be able to perform all the actions (device level as well as certificate level).

Functional Specification

Basic information specifications

- Users should be able to provide basic information such as Account name, Device description, and Account number.
- The account name should be maintained as a unique factor; the user should not be allowed to add the same account name more than once.
- When the user tries to submit the same Account name, a pop-up error message displays as **Account name already available in the inventory**.

Account name

- The account name is a mandatory field. Users should provide a valid name in this column.
- The account name field should be an alphanumeric field. Users should be able to provide alphabets and numbers.
- Users should not be able to provide any special characters in this field, except period (.)
- Users should not be able to provide [space] in this field.
- The account name field should support only 25 characters. Block users to enter more than 25 characters.
- Add an information icon next to the account name text box and displays a message as **Account name should be unique**. The account name already in the cloud inventory cannot be added again. Only alphanumeric and period (.) can be entered in this field.

Description

- Users can provide the description in this paragraph box.
- Allow a maximum of 250 characters in the description field.
- Allow numbers, alphabets, all the special characters, and [space] in the description field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Account number

- The account number is an optional field. Users should provide a valid account number in this column.
- Users should be able to enter only numbers in the account number.
- Users should not be able to provide any special characters or empty spaces in this field.
- Users should be able to provide a maximum of 25 numbers. Users should not be able to provide more than 25 entries.

Proxy required

- Proxy required is an optional field, when the user selects this checkbox, AppViewX will try to communicate via Proxy in case of network failure/absence.
- If the user does not select this checkbox, then AppViewX will connect/communicate only via the internet/network, if there is network failure/absence, AppViewX will not try to communicate via provided Proxy.

Credentials Specifications

- Only when the master credential is selected in the above section, the **Credential** section will be displayed in this form. When the user lands on this page to add a new cloud device, by default, the master credential will be selected, hence the **Credential** section will be displayed as well.
- Users should be able to provide the credentials in this section; if the master credential is selected against the credential type. It should be used to access all the services that are selected in the services section.

Credential input type

- The credential input type is a mandatory field. It is a single select dropdown. By default, **Manual Entry** will be displayed.
- Credential input type should list three options, they are
  - Manual entry
  - Credential list – CyberArk
  - Credential list – AppViewX
- When **Manual Entry** is selected, **Access Key** and **Secret key fields** should bedisplayed below Credential input type fields.
  - The access key and secret key are mandatory fields and Password encrypted fields.
  - Users should provide both access key and secret key corresponding to the account added.
  - These keys will be used to access all the services that are selected in the services section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- When **Credential List – CyberArk** is selected, the **Credential list dropdown** should be displayed below the **Credential type** field.
  - Users should be able to select a credential that is saved in CyberArk. This credential will be used to access all the services that are selected in the services section.
- When the **Credential list – AppViewX** is selected, the **Credential list dropdown** should be displayed below the **Credential type** field.
  - Users should be able to select a credential that is saved in AppViewX vault. This credential will be used to access all the services that are selected in the services section.

Access key

- When the user lands on this page to add a new cloud device, by default, Manual Entry will be displayed under the Credential input type. Hence, the Access Key field will be displayed as well.
- The access key is a mandatory, password-encrypted, and alphanumeric field. Users should be able to provide alphabets as well as numbers in this field.
- All the special characters should be supported in this field.
- Users should not be able to enter empty spaces in this field.
- The minimum and maximum length of the access key is 16 and 128 characters respectively.

Secret key

- When the user lands on this page to add a new cloud device, the manual entry will be displayed under the credential input type. Hence, the secret key field will be displayed as well.
- The secret key is a mandatory, password-encrypted, and alphanumeric field. Users should be able to provide alphabets as well as numbers in this field.
- All the special characters should be supported in this field.
- Users should not be able to enter empty spaces in this field.
- The maximum length of the secret key is 256 characters.

Key information specifications

- Users should be able to provide the key information such as the **datacenter**, **region**, **credential type**, and **account number**.
- Users have to provide a data center, region, and service. If any of these fields are empty, while submitting the form, the X mark will be displayed against the field that is not filled. A message will be displayed when the user mouse over the X mark, “Value is missing in <*fieldName*> field”.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Data Center

- **Data center** is a mandatory field, the **Select a data center** message must be displayed as a play holder when the user lands on this page to add a new cloud device.

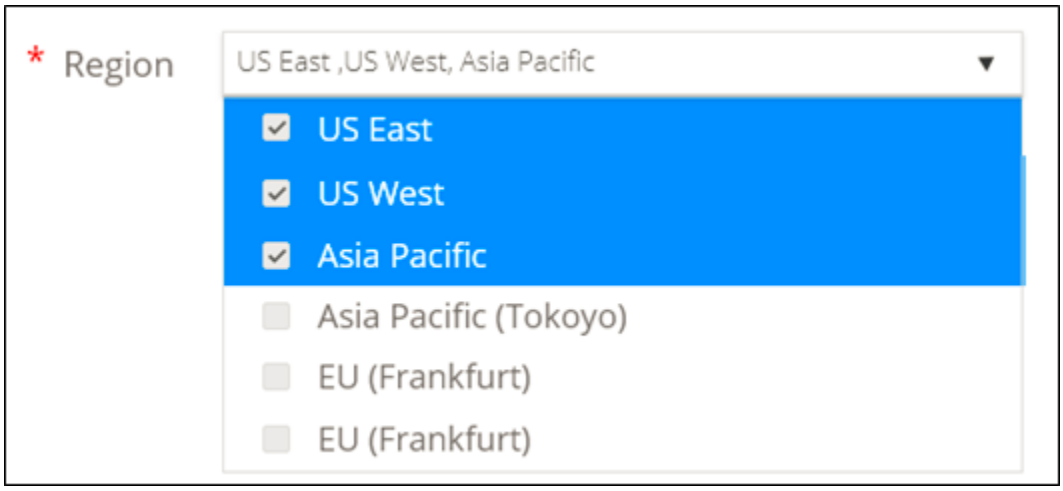
- Users can select a data center for the dropdown (single select dropdown).

- Based on the data center selected, the region corresponding to the selected data center will be listed below the field region field.
- Users should be restricted to submit this form, without filling a data center. If the user does not select a data center, while submitting the form, X mark will be displayed against the data center field. A message will be displayed when the user mouse over X mark, “Value is missing in datacenter field”.

Region

- Region is a mandatory field.
- Fetch region(s) button will be enabled only when the credentials are given. The user should provide the credentials to enable the fetch region(s)
- Once credentials are provided, the fetch region(s) will be enabled. Users should be able to click the fetch region(s) button.
- Once the user click fetch region(s) by providing valid credentials, a list of all the regions corresponding to the credential provided will be displayed in the drop-down,
- If provided credentials do not have any region (or) if the provided credential is invalid, then None will be displayed in the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- The **Select the region(s)** message must be displayed as a play holder when the user lands on this page to add a new cloud device.
- Users can select single or multiple regions from this dropdown (multi-select dropdown).
- Users should be able to select all / unselect all the regions from this field.
- Users should be able to free-text search the region in the dropdown.
- Users should be restricted to submit this form, without selecting at least one region. If the user does not select a region, while submitting the form, the X mark will be displayed against the region field. A message will be displayed when the user mouse over X mark, **Value is missing in region field**.

Service

1. Service is a mandatory field. It is a multi-select text box. By default, **ACM** and **IAM** will be selected.

2. Users can select single or multiple service(s) from this dropdown (multi-select text box).
3. ACM, IAM, ELB, and EC2 are the services that should be listed in the dropdown.
4. AppViewX should support four Amazon AWS services, they are, ACM, IAM, ELB, and EC2 instances. Users should be able to select any one of these services from this field.
5. Based on the selected service, the user should provide additional details in the below section.
6. Users should be able to select all / unselect all the services from this field.
7. Users should be able to free-text search the service from this field.
8. Users should be restricted to submit this form, without selecting at least one service. If the user does not select a service, while submitting the form, X mark will be displayed against the service field. A message will be displayed when the user mouse over X mark, **Value is missing in-service field**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Additional Attributes Specifications

Service Input Status

- The services that are selected in the services section will be displayed as a tab in this section.
- Each tab will have a different set of fields that are required for accessing each service.
- There are a few mandatory fields corresponding to each service.
- When the user lands on this page to add a new cloud device, by default, **ACM** and **IAM** tabs will be displayed.
- Once mandatory fields are filled, each tab will be indicated with a GREEN tick mark. Only when all the selected services are marked with a GREEN tick, the user will be able to submit the form.
- If the user tries to save without filling in the required detail, an **X** mark should be displayed against each tab that is not completed.
- When the user mouse over **X**mark below message should be displayed, “Mandatory fields are not filled in this tab”

Cert sync

- Cert sync is a mandatory field. When the user lands on this page to add a new cloud device, by default, Managed will be selected.
- Cert sync should be available in all the tab.
- Cert sync have three options,
  - **Managed**: Certificates within the cloud (corresponding to the service selected), & its objects will be discovered and moved to inventory with managed status. Users can perform different AppViewX actions on the certificates that are in managed status. For example, cert sync in the ACM tab is selected as **Managed**, then all the certificates in ACM will be discovered and moved to the inventory with managed status.
  - **Monitored**: Certificates within the cloud (corresponding to the service selected), and their objects will be discovered and moved to inventory with monitored status. Users can only monitor the certificates that are in monitored status, user cannot perform any AppViewX actions on these certificates. For example, cert sync in the ACM tab is selected as **Monitored**, then all the certificates in ACM will be discovered and moved to the inventory with monitored status.
  - **Ignored**: The cloud account will be added and managed in AppViewX. Certificates within the cloud (corresponding to the service selected), & its objects will **not** be discovered; only the profiles will be created.

Collection type

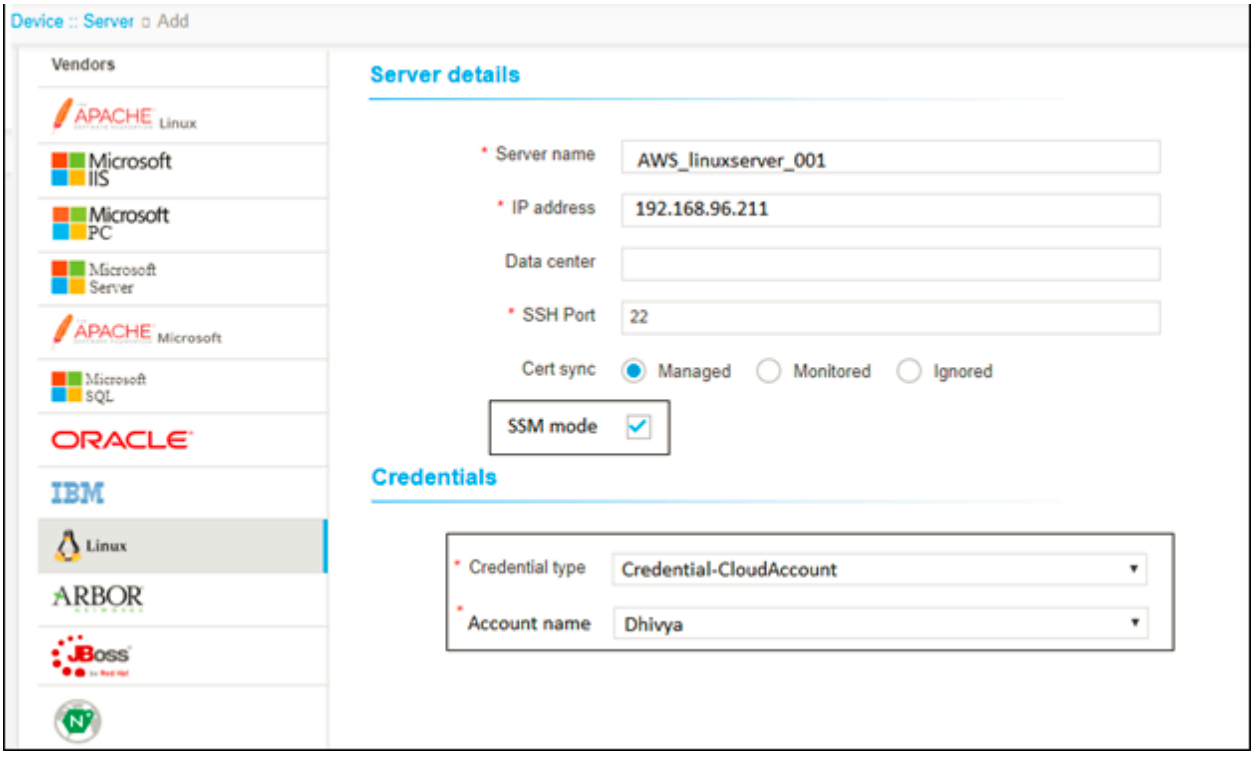
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. The collection type field will be displayed only when the EC2 option is selected under the service section.
2. Collection type is an optional field.
3. All the regions selected by the user should be listed in the collection type section.
4. Users should be able to select a single S3 bucket for all the regions, also users should be able to select an individual S3 bucket for each region.
5. Data stored in S3 must be removed instantly.

Generic Linux SSM Integration Specification

Device Addition

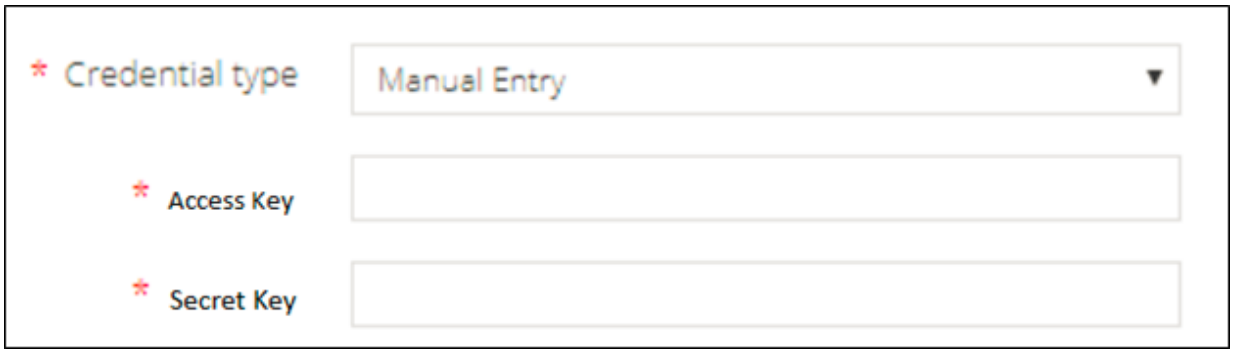
- ApartfromApache, all other instances identifiedfrom Amazon EC2 should be added under Generic Linux under the Server tab in AppViewX.
- All the mandatory fields should be pre-fill on the Generic Linux device addition page.
- The server name should be appended with AWS as shown below.
- By default, the communication mode should be selected as **SSM.**
- Credential provided in cloud inventory should be used in server inventory as well.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credential management

- Credential Type is a mandatory field.
- When a device is added from a Could account, **Credential-CloudAccount must** be displayed corresponding to a credential type label. And the cloud account name should be displayed in a dropdown corresponding to the Account name label.
- While modifying the mandatory details in the Generic Linux form, the user should be able to select a different cloud account credential that is added to the cloud inventory.
- Similarly, while modifying the mandatory details in the Generic Linux form, the user should be able to provide credentials manually in the Generic Linux device addition form.



- Only when the mode of communication is SSM, Access key, and Secret key fields will be displayed under Credential type.

Instances Discovery Specification

Specifications

- It is mandatory for the user to provide credentials and S3 bucket details to identify instances within the Amazon EC2 service.
- With details provided, AppViewX should be able to identify Apache (Linux) server within the Amazon EC2 service and all other instances within the EC2 service will be mapped to Generic Linux in the server tab.
- AppViewX uses the SSM mode of communication to discover certificates within these instances.
- If multiple Apaches run in the same EC2 instance, then only one account will be added under the Apache server tab; if multiple apache running in different EC2 instances; then each instance (apache) will be added as a different account under the Apache server tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- All the certificates within these instances should be discovered by AppViewX, when the **Cert sync** field is selected as **Managed**/ **Monitored**.
- Should not support push certificates including private key via SSM. CSR must be generated in the device itself only a signed public key should be pushed to the device.

Delete Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Delete**) icon in the command bar.
   The **Delete** confirmation popup window is displayed.
5. Click **Yes**.
   The cloud will be removed from the device inventory.

Import Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Import**) icon in the command bar.
   You will be redirected to the import cloud page.
5. Download the sample <.csv> or <.xls> file.
6. Update the details.
7. Click the browse and upload button.
8. Upload the files.
   Cloud details will be updated to the firewall inventory.

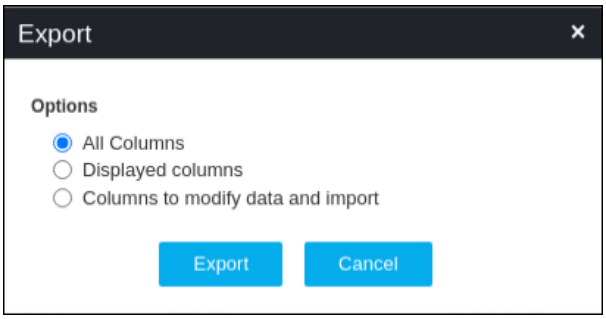
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Export Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the **Export** icon in the command bar at the upper right of the screen.
5. On the **Export** pop-up screen that is displayed, select the type of information you want to export:



   a. **All Columns** - Select this option if you want to export all information about the cloud.
   b. **Displayed columns** - Select this option if you want to export only the information that is visible on the cloud screen.
   c. **Columns to modify data and import** - Select this option if you are exporting firewall details to make modifications and then re-import the data into the cloud inventory.
6. On the screen that opens, select the location where you want the cloud details file to go, then click **Save**.
   Cloud details will be downloaded as an Excel `<.xls>` file.
7.

Manage Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If the desired server device is not listed on the screen, run a search.

4. To start managing the cloud, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   - Config fetch will be triggered and the cloud will get managed.
   - Cloud status is changed to **Manage** in Cloud inventory.

Note: With the introduction of the **Cert License Enforcement**; Server Auto discovery of EC2 instances will be on-boarded with certs status as **Monitored**, even if managed state is configured in the Cloud account configuration.

Unmanage Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

Note: If the desired server device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   Cloud device status is changed to UnManaged in Cloud inventory.

Fetch Config for Cloud

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Cloud** tab.
3. Click the check-box beside the device name.

Note: If the desired server device is not listed on the screen, run a search.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Click the (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the cloud.** The configuration will be fetched from the server.

Configuring WAFs

- Adding a WAF Device
- Deleting a WAF Device
- Importing a WAF Device
- Exporting a WAF Device
- Managing a WAF Device
- Unmanaging a WAF Device
- Fetching Config for WAF Devices

Adding a WAF Device

AppViewX supports integration with the following WAF vendors:

- Barracuda
- Cloudflare
- F5
- Imperva SecureSphere

- Adding Barracuda
- Adding Cloudflare
- Adding F5
- Adding Imperva SecureSphere

Adding Barracuda

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Device details** page is displayed.

4. Select **Barracuda** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
Platform	Select the platform from the dropdown field • Azure • AWS • On-Prem
***Device name**	Enter a unique name for the device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the device to be onboarded.
***Rest port**	Enter the rest port number.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the Barracuda. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for Barracuda.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access Barracuda.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

7. In the **Secondary device information** section, select/enter the details as follows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Secondary / Alternate device	Select either *Auto-detect* or *Manual entry*.
***Device name**	Enter a unique name for the secondary device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the secondary device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the secondary device to be onboarded.
***Rest port**	Enter the rest port number of the secondary device.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
**: Mandatory fields*	

In the **Secondary device credentials** section (displayed only if **Secondary / Alternate device** = **Manual entry** select/enter the details as follows.

Fields	Description
***Use same credentials**	The *Enable* checkbox is used to fix the credentials type to either *Credential List - Appviewx* or *Credential List - CyberArk* based on its selection.
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the secondary device. API is the default value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for the secondary device.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access the secondary device.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

8. (*Optional step*) Click **Add**. This button is displayed only if **Secondary device information** is **Manual entry**. More than one devices can be configured. (use the **Update** and **Delete** buttons to make changes or remove the devices added.)
9. Click **Save**.
   The device is onboarded successfully.

Adding Cloudflare

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Device details** page is displayed.

4. Select **Cloudflare** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
***Account name**	A user defined unique name to identify the server. No special characters other than '-' , '_' , '.' , '*' , '|' , '!' and spaces are not allowed.
Data center	Enter the data center routing. It holds all the SSL related information that is to be retrieved from the Cloudflare device.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the Cloudflare.
***Token based Authentication**	Select the checkbox to enable the token based authentication.
API Token	Enter the API token if the token based authentication is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Username**	This field will be visible if the Credential Type is selected as **Manual entry and token based authentication is disabled** . Enter the designated username for Cloudflare.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry and token based authentication is disabled** . Enter the designated password to access Cloudflare.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

7. Click **Save**.
   The device is onboarded successfully.

Adding F5

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **f5** from the Vendors list.
5. In the **General Information** section, select/enter the details as follows.

Fields	Description
Platform	Select the platform from the dropdown field. ASM is the default value.
***Device name**	Enter a unique name for the device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the IP address of the device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the device to be onboarded.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the F5 device. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for Barracuda.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access Barracuda.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
***Token based authentication**	Select the checkbox to enable the token based authentication.
**: Mandatory fields*	

7. In the **Secondary device information** section, select/enter the details as follows.

Fields	Description
Secondary / Alternate device	Select either *Auto-detect* or *Manual entry*.
***Device name**	Enter a unique name for the secondary device to be onborded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the secondary device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the fully qualified domain name of the secondary device to be onboarded.
***Rest port**	Enter the rest port number of the secondary device.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
**: Mandatory fields*	

In the **Secondary device credentials** section (displayed only if **Secondary / Alternate device** = **Manual entry** select/enter the details as follows.

Fields	Description
***Use same credentials**	The *Enable* checkbox is used to fix the credentials type to either *Credential List - Appviewx* or *Credential List - CyberArk* based on its selection.
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the secondary device. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for the secondary device.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access the secondary device.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

8. (*Optional step*) Click **Add**. This button is displayed only if **Secondary device information** is **Manual entry**. More than one devices can be configured. (use the **Update** and **Delete** buttons to make changes or remove the devices added.)
9. Click **Save**.
   The device is onboarded successfully.

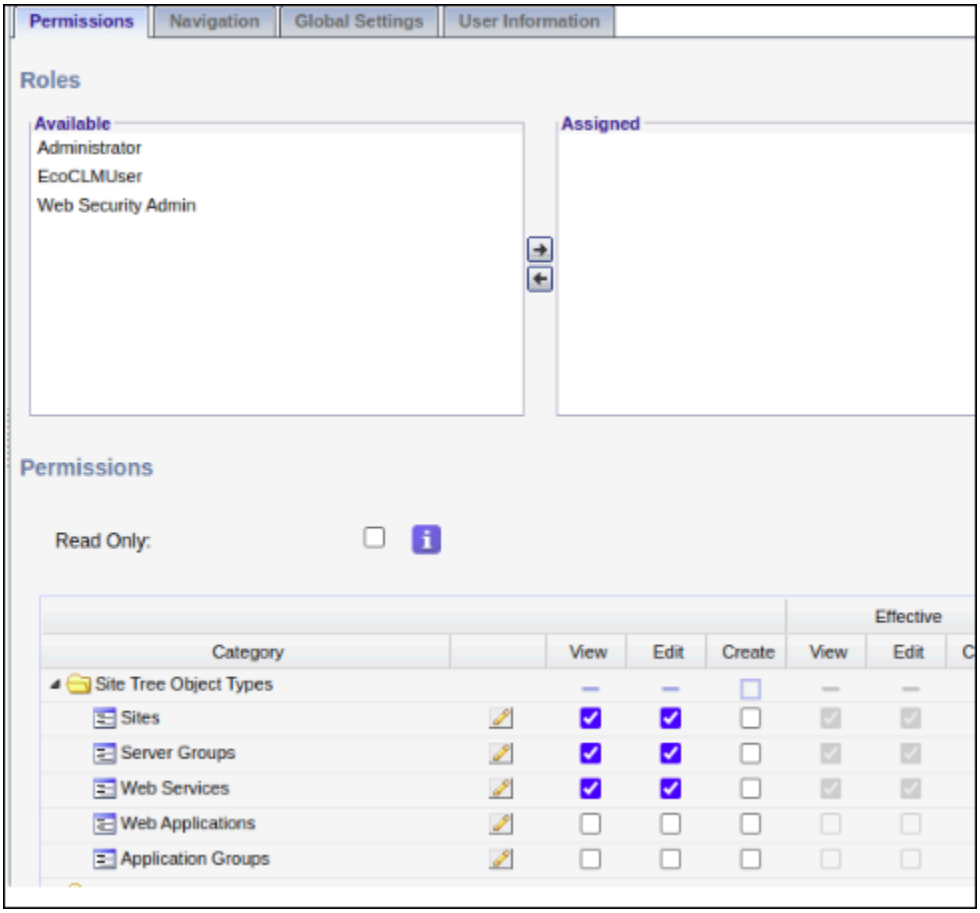
Adding Imperva SecureSphere

Prerequisites

- **AWS**
  - User permissions and navigation settings can be configured either individually or by assigning a predefined role that includes the necessary settings. When a role is assigned, the user automatically inherits all privileges associated with that role. While additional permissions or navigation options can be added, privileges inherited from the role cannot be revoked individually.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Minimum required permissions**



In the **Site Tree Object Types** category, enable:

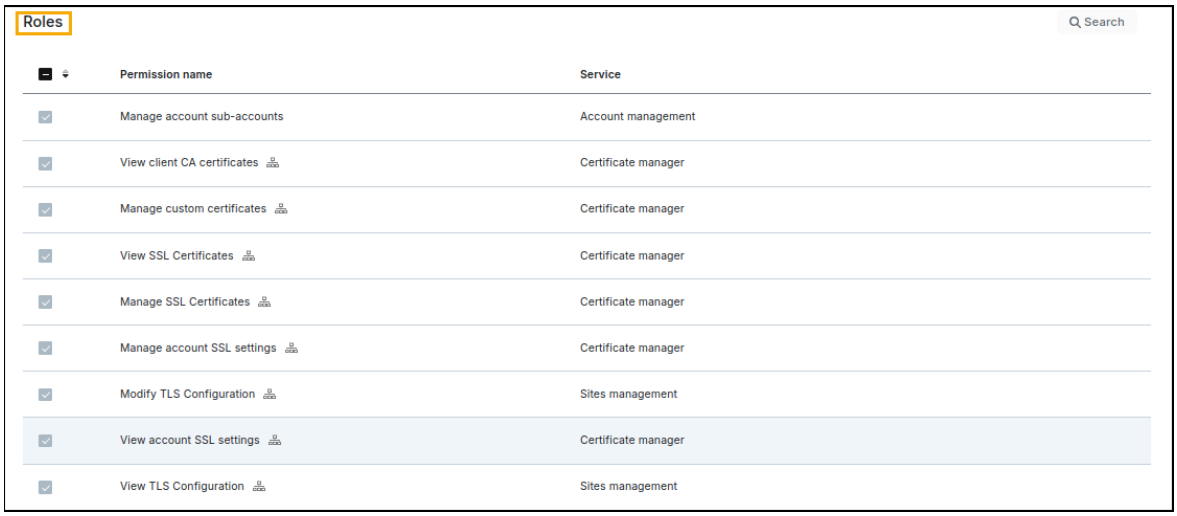
- Sites > Edit
- Server Groups > Edit
- Web Services > Edit

Note: Edit access provides View/Read access implicitly; no need to provide View access separately.

- **SaaS**
  - Configure user account roles and permissions within Imperva SaaS to efficiently perform Certificate Lifecycle Management (CLM) operations. Enable administrator or service account access to the Imperva SaaS portal to create a new User and role.
  - Define and manage roles to assign the appropriate permissions for Imperva SaaS configuration sync, endpoint enrollment, push, and binding from AppViewX to Imperva SaaS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Access the Roles page to create and manage roles. This page is available to the account administrator or users with the **Manage user roles** permission.
  1. On the sidebar, click **User Management** > **Roles** > **New Role**.
  2. Create a new role with the following permissions:



Permissions:

- View client CA certificates
- Manage custom certificates
- Manage account SSL settings
- View account SSL settings
- View TLS Configuration
- View SSL Certificates
- Manage SSL Certificates
- Modify TLS Configuration
- Manage account sub-accounts

Limitations

- **AWS**
  - Due to API limitations, existing certificates from Imperva AWS/On-Prem cannot be discovered. Furthermore, the discovery API metadata does not include the certificate's serial number, which prevents the creation of an AppConnector for the discovered certificate.
  - CSR generation is not supported at the endpoint.
- **SaaS**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Imperva SaaS does not offer an API for exporting certificate content and only provides certificate metadata. Consequently, certificates from Imperva SaaS cannot be directly discovered. However, if a certificate is already present in the AppViewX inventory, a connector will be created using the serial number from the metadata.

API Key Management

To use the API, the client must be authenticated by Imperva.

1. On the sidebar, click **User Management** > **Users**.
2. Click **Add New user** to create a new user, and then enter the details as required.
3. Click the **Add User** button.

> **Note:** When a new user is added to an account, a verification email is sent to their registered address. The user must click the link in the email to verify their address and set a login password.

4. Once the User account is created, select **Edit**, navigate to the **API Keys** category, and generate an API ID and API Key.
5. Click **Create**. It creates an API ID and API Key.

> **Note:** Copy the API key now as it will no longer be accessible once you close this window.

To add the WAF device:

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Imperva Securesphere** from the Vendors list.
5. In the **General Information** section, enter the details as follows:

Fields	Description
Platform	Select either: • **AWS**: Select **AWS** for Imperva on-prem or AWS Marketplace deployment. • **SaaS**: Select **SaaS** for Imperva SaaS deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: By default, **AWS** platform is selected.
***Device name**	Enter a unique name for the device to be onboarded.
Communication	This field is displayed if **Platform = AWS**. Select *IP address* or *FQDN*.
***IP Address**	This field is displayed if **Platform = AWS** and **Communication = IP Address**. Enter the IP address of the device to be onboarded.
***FQDN**	This field is displayed if **Platform = AWS** and **Communication = FQDN**, or if **Platform = SaaS**. Enter the fully qualified domain name of the device to be onboarded.
***Rest port**	This field is displayed if **Platform = AWS**. Enter the rest port number.
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
Proxy Required	Enable this field if the device communication needs to happen via a proxy. The proxy details configured in general settings will be used for communication.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Note: AppViewX supports certificate enrollment and deployment to the primary Imperva SaaS account and its associated sub-accounts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the WAF device.

Note: This field is displayed if **General Information** = **AWS**.

Fields	Description
***Credential Type**	Select the credential type from the dropdown: • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - AppVewX* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the Imperva SecureSphere. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for Imperva Sourcesphere.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated password to access Barracuda.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

Note: This field is displayed if **General Information** = **SaaS**

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box.
***Access type**	Select the method to access the Imperva SecureSphere. API is the default value.
***API ID**	Enter the valid API ID.
***API Key**	Enter the valid API ID.
*: Mandatory fields	

7. In the **Secondary device information** section, enter the details as follows.

Note: This field is displayed if **General Information** = **AWS.**

Fields	Description
Secondary / Failover / Sync group	Select either *Ignore* or *Manual entry*.
***Device name**	Enter a unique name for the secondary device to be onboarded.
Communication	Select from *IP address* and *FQDN*.
***IP Address**	This field is displayed if **Communication = IP Address** Enter the IP address of the secondary device to be onboarded.
***FQDN**	This field is displayed if **Communication = FQDN** Enter the fully qualified domain name of the secondary device to be onboarded.
***Rest port**	Enter the rest port number of the secondary device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Enter the data center name. It holds all the SSL related information that is to be retrieved from the server.
**: Mandatory fields*	

In the **Secondary device credentials** section (displayed only if **Secondary / Alternate device** = **Manual entry** enter the details as follows.

Fields	Description
***Use same credentials**	The *Enable* checkbox is used to fix the credentials type to either *Credential List - Appviewx* or *Credential List - CyberArk* based on its selection.
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) - to directly add the credentials in the username and password text box. • *Credential List - Appviewx* - to use any credentials from the saved AppViewX Credential List. • *Credential List - CyberArk* - to use any credentials from the saved AppViewX CyberArk List.
***Access type**	Select the method to access the secondary device. API is the default value.
***Username**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the username is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed. Enter the designated username for the secondary device.
***Password**	This field will be visible if the Credential Type is selected as **Manual entry**. If the Credential Type is selected as **Credential List - Appviewx**, the password is entered by default and field is read only. If the Credential Type is selected as **Credential List - Cyerark**, this field is not displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the designated password to access the secondary device.
***Credential list**	This field will be visible only if the Credential type is selected as **Credential List - AppViewX** or **Credential List - CyberArk** The dropdown contains a list of credentials stored in AppViewX.
**: Mandatory fields*	

8. [Optional step] Click **Add**. This button is displayed only if **Secondary device information** is **Manual entry**. More than one devices can be configured. (Use the **Update** and **Delete** buttons to make changes or remove the devices added.)
9. Click **Save**.
   The device is onboarded successfully.

Deleting a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name.

> **Note:** If the desired server device is not listed on the screen, run a search.

4. Click the (**Delete**) icon in the command bar.
   The **Delete** confirmation popup window is displayed.
5. Click **Yes**.
   The firewall will be removed from the device inventory.

Importing a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If the desired server device is not listed on the screen, run a search.

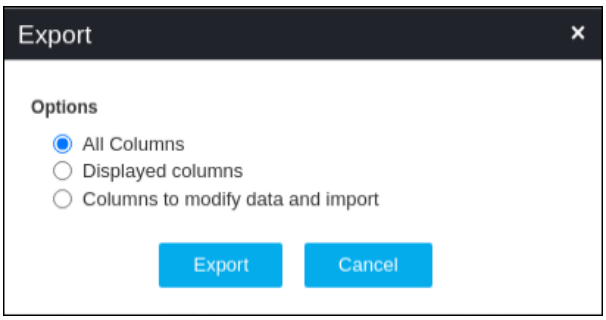
4. Click the (**Import**) icon in the command bar.
   You will be redirected to the import page.
5. Click **Browse** to navigate to the location of the file to be uploaded.
6. Once the file is selected, click **Upload**.
7. Click **Submit**.

Exporting a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the check-box beside the device name. If you are exporting details of multiple devices, select the check-boxes for each one.

Note: If the required device is not listed on the screen, run a search.

4. Click the (**Export**) icon in the command bar at the upper right of the screen.
5. On the Export pop-up screen that is displayed, select the type of information you want to export and click the **Export** button.



   a. **All Columns** - Select this option if you want to export all information about the firewall.
   b. **Displayed columns** - Select this option if you want to export only the information that is visible on the firewall screen.
   c. **Columns to modify data and import** - Select this option if you are exporting firewall details to make modifications and then re-import the data into the firewall Inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. On the screen that opens, select the location where you want the firewall details file to go, then click **Save**.
   Device details will be downloaded as a **.xls** file.

Managing a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the checkbox beside the device name.

> **Note:** If the required device is not listed on the screen, run a search.

4. To start managing the device, click the (**Manage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation pop-up message that is displayed.
   - Config fetch will be triggered and the device will get managed.
   - Device status is changed to **Manage** in the inventory.

Unmanaging a WAF Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the checkbox beside the device name.

> **Note:** If the required device is not listed on the screen, run a search.

4. Click the (**Unmanage**) icon in the command bar at the top of the screen.
5. Click the **Yes** button from the confirmation popup message that is displayed.
   Device status is changed to **UnManaged** in the inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fetching Config for WAF Devices

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **WAF** tab.
3. Click the checkbox beside the device name.

> **Note:** If the required device is not listed on the screen, run a search.

4. Click the (**Fetch Config**) icon in the command bar.
   A popup notification message is displayed as **Fetch config has been triggered for the device(s).**
   The configuration will be fetched from the server.

Certificate Reports

Once the certificates are discovered and managed/monitored in AppViewX, those certificates can be viewed as the reports in dashboards. For some of the reports, email notifications can be enabled as well provided with the other functionality as downloading the report/data.

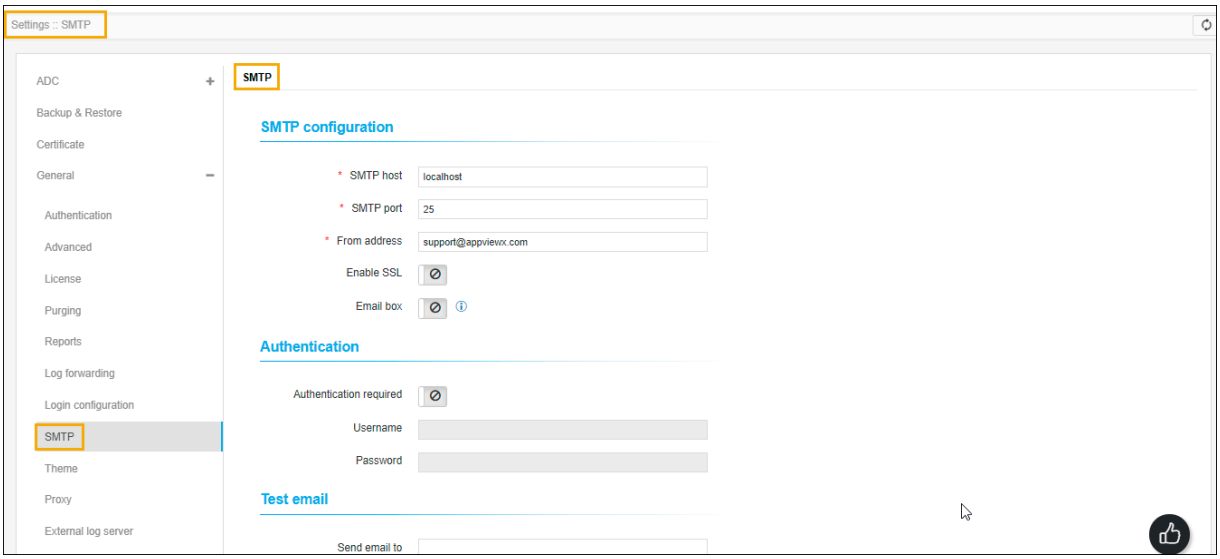
> **Note:** Default reports will contain data only if there is at least one relevant certificate present for that report in the inventory. Otherwise, it displays pop-up message as **No Records Found**.

SMTP Configuration

To get the certificate reports sent as a mail, we will have to first configure SMTP

1. Log in to the AppViewX application with valid credentials.
2. Click on the menu button.
   The left navigation pane is displayed.
3. Click **Settings.**
   The **Settings** page is displayed.
4. Expand the General menu and then click **SMTP.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. Refer to the fields in the table below to update the information on the SMTP page.

SMTP Page - Field Description Table

Name	Type	Description	Error Message
* SMTP host	Text	The server that will send the email.	Enter valid Hostname/ IP address <x.x.x.x>.
* SMTP port	Text	Port to connect to the email server.	• Port can contain only numbers. • Enter a port number between 0-65535.
* From address	Text	Mail address from which mail is to be received by the user.	• Please enter a valid email.
Enable SSL	Toggle button	To enable/disable SSL while sending mail.	NA
Email box	Toggle button	Enabling this setting will use IMAP for the mailbox.	NA
* Email	Text	Email for IMAP. Mandatory if Email box is enabled.	• Please enter a valid email.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

SMTP Page - Field Description Table (continued)

Name	Type	Description	Error Message
Password	Text	Password for IMAP. Mandatory if Email box is enabled.	This field is mandatory.
* Hostname	Text	The hostname for IMAP. Mandatory if Email box is enabled.	• Enter valid Hostname/ IP address <x.x.x.x>.
Authentication required	Toggle button	To enable/disable Authentication required.	NA
* Username	Text	The username if authentication required. Mandatory if Authentication required is selected as true.	NA
* Password	Text	Mandatory if Authentication required is selected as true.	NA
* Send email to	Text	Test email to check if able to send mail after configuring the above settings. Mandatory if you want to test.	Enter a valid email.

Note: The asterisk (*) symbol indicates a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

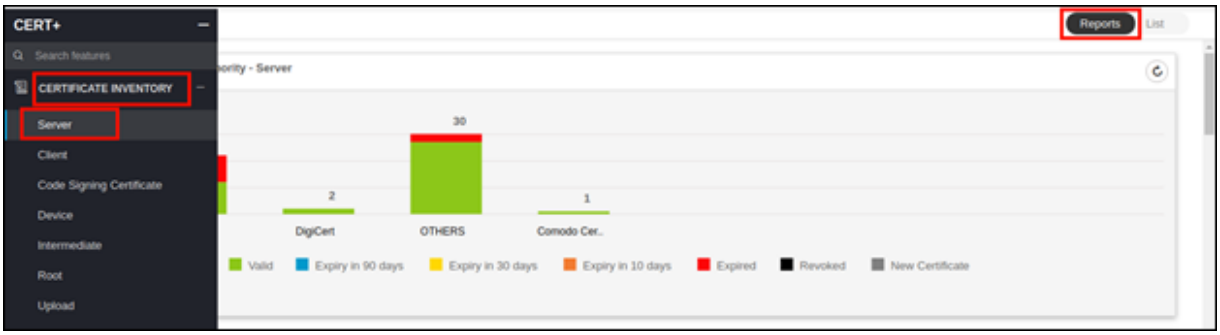
Troubleshooting SMTP

Error Message	Possible Cause	Possible Solution
Please provide a valid value.	Anyone of the mandatory fields is invalid or is missing.	Provide valid values for all mandatory fields.
E-Mail sending was unsuccessful.	• If trying to test, no/valid email is not provided in the 'send email to' field. • Credentials and field values may be incorrect.	• If trying to test, provide a valid email in the 'send email to' field. • All the credentials and fields should be correct.
Service unavailable. Try after some time.	avx_subsystems or avx_platform_gateway is not running.	Restart the plugin.

Fetch All Default Reports

All Reports will be present separately for each certificate category. To view Reports for certain certificate categories, follow the steps given below.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server** or **Client** or **Code Signing Certificate**.
2. In the top right corner, click **Reports** tab.
   The respective report page is displayed.



Working with the Job Scheduler

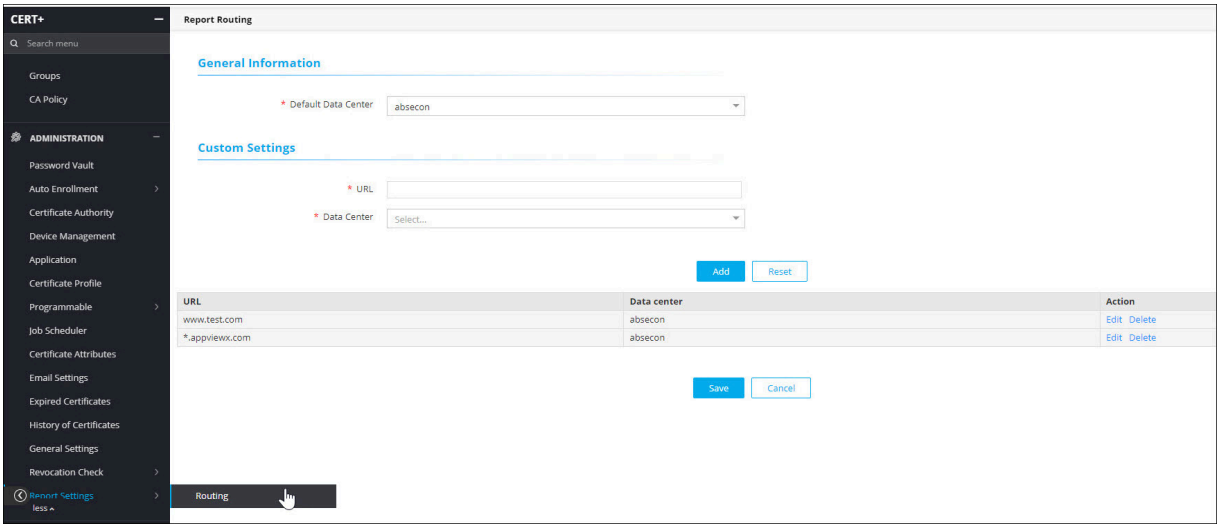
Report Routing

This functionality is applicable only to the following reports:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Validation report
- Vulnerability report
- CAA report

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Report Settings** > **Routing** or **Code Signing**. The **Report Routing** page is displayed.



2. Enter the following fields:

Revocation Routing Page - Fields Description

Fields	Description
General Information	
Default Data Center	This is the default data center through which all validation requests are routed.
Custom Settings	
URL	Type the URL of the certificate for which you want to perform the revocation check.
Data Center	Select the data center of the URL from the dropdown list. Selecting this value will overwrite the default data center.

Note: The asterisk (*) symbol indicates a mandatory field.

3. Click **Add.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The table is refreshed with a row entry of the newly added URL and the data center.

4. Click **Save.**
   - A message that certificate report settings routing is saved successfully is displayed.
   - On saving, any report validation such as validation checks or CAA record check is routed through the data center configured on this page.

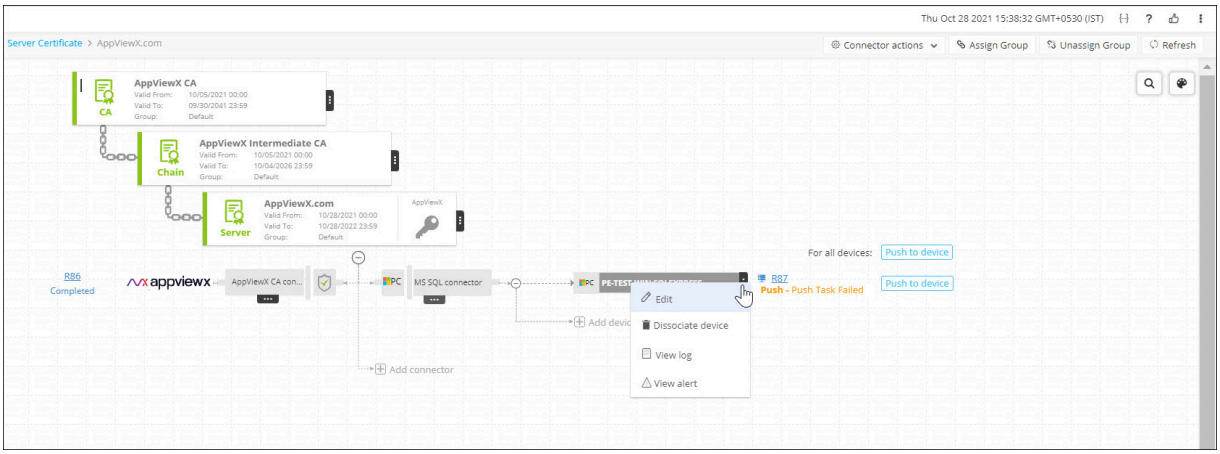
> **Note:** To perform a bulk operation on certificate URLs, you can specify a wild card character with their domain name, for example, if you want to specify a data center to all the AppViewX certificates at one go, then use wild card character as in *.appviewx.com and select the data center from the dropdown list.

5. Click **Add**.
6. To edit the certificates, then use the **Edit** option.

Validation Settings

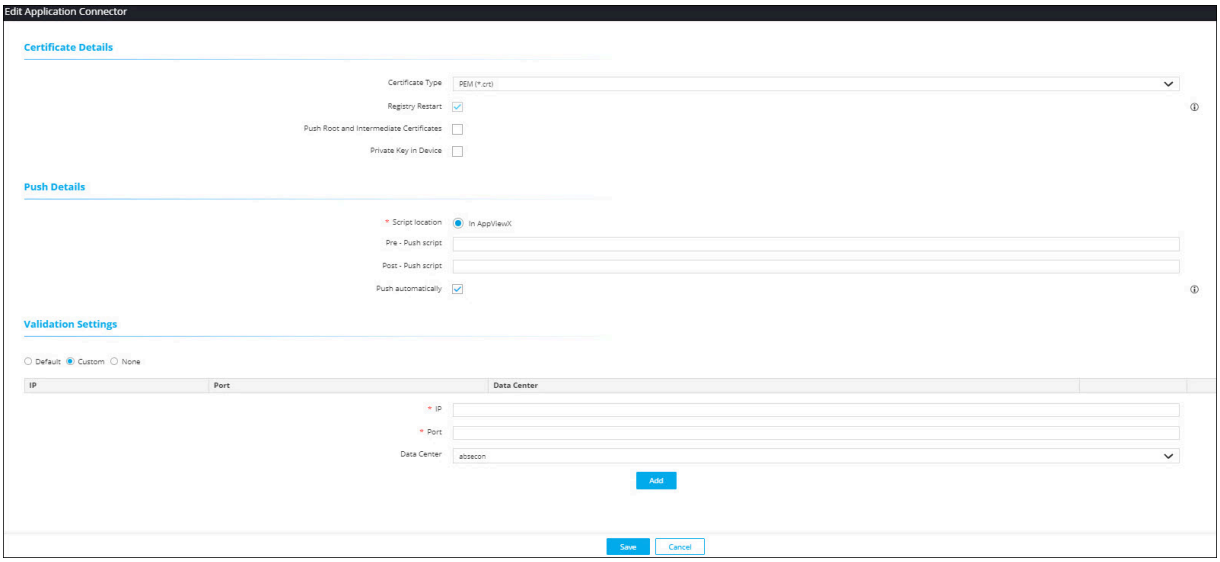
This is an extended feature of Report Routing.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server** or **Client** or **Code Signing**.
2. Click the **Common Name** link to view the certificate in the holistic view.
3. Hover the mouse over the (**More**) icon of the application connector and click **Edit.**



The **Edit Application Connector** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



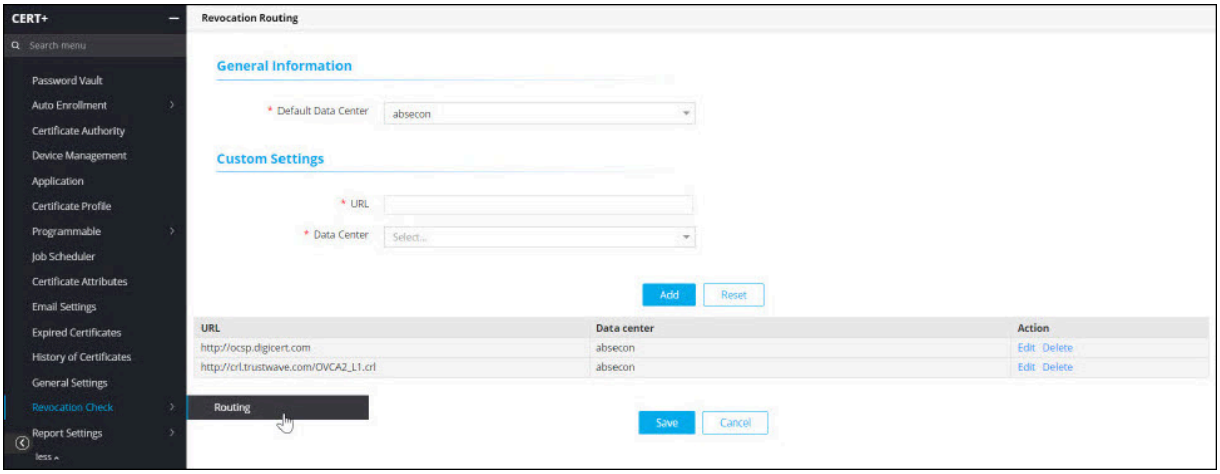
4. Select **Custom** option.
5. In the **Validation Settings** section, select the data center from the dropdown list.
   This ensures that for any validation check, this is treated as high priority.

Revocation Check Routing

This functionality is applicable to:

- Revocation check job
- On demand revocation check

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Revocation Check** > **Routing** .
   The **Revocation Routing** page is displayed.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Enter the following fields:

Revocation Routing Page - Fields Description

Fields	Description
General Information	
***Default Data Center**	This is the default data center through which all validation requests are routed.
Custom Settings	
***URL**	Specify the URL for which you want to run the revocation check job or the on-demand revocation check by selecting the certificate from the holistic view. To run the revocation check job, copy and paste the URL from the **CRL distribution points** field of the **Certificate details** window. To run the on demand revocation check, copy and paste the URL with ocsp extension from the **Authority information access** field of the **Certificate details** window. **Note:** For on demand revocation checks, if you have configured two URLs with .crl and .ocsp extensions and for any reason the job fails on .ocsp, then the revocation check is triggered on the URL with .crl extension. If the job is successful and the certificate is revoked, then the certificate is displayed on the **Certificate Inventory** page with a black icon against it. If the job failed, then go to **Administration > Logging > Certificate** and check the log message.
***Data Center**	Select the data center of the URL from the dropdown list. Selecting this value will overwrite the default data center.
Note: The asterisk (*) symbol indicates a mandatory field.	

3. Click **Add**.

   The table is refreshed with the added URL and the data center.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Click **Save**.
   - A message that certificate revocation check routing is saved successfully is displayed.
   - The table is refreshed with a row entry of the newly added URL and the data center.

Securing CERT+

CERT+ Certificate Lifecycle Management (CLM) offers capabilities to discover and manage certificates on devices and self-service certificate enrollment for users. CERT+ also acts as a Key Escrow for keys discovered and enrolled.

Typically, the private keys are stored by the devices handling SSL termination, and an SSL management tool retrieves them during certificate renewal. The tools and devices store them in their storage in the original format, which can be reused. If there is an attack on the device or tool storage, the private keys will be given away, which can be used to host an array of attacks.

AppViewX stores the private keys discovered in a secure part of the database, which is encrypted using the AES-256 algorithm. It encrypts each private key with independent keys and stores the encrypted independent keys in the database with a randomly generated key.

Thus, even if the hackers get the database, they will not be able to get the private keys. Only a maze of jumbled up characters will be visible to them, which does not make any sense and hence, rendering the attack useless.

Auto-Enrollment Protocols

AppViewX CERT+ enables certificate auto-enrollment by automating all the steps involved, including CSR generation, domain ownership verification, certificate download, and provisioning, making the process efficient, scalable, and secure. AppViewX CERT+ supports all major auto-enrollment protocols including – ACME, EST, SCEP, Native Windows Auto-enrollment, and Microsoft Intune. Automating certificate enrollment reduces human error, outages, and security compromises, while improving productivity.

Auto-enrollment protocols are standardized enrollment mechanisms accepted across a wide range of enterprise systems for device and application certificate enrollment. Systems leveraging auto-enrollment protocols typically expect minimum to no admin intervention. Network devices such as routers-switches, DevOps tools, and Enterprise Mobility Management platforms are typical examples of such systems. If the deployment mode is:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- SaaS or Managed Kubernetes, deploying a cloud connector enables auto-enrollment.
- SaaS deployments where cloud connectors are unavailable, users should provide the AppViewX host information, which includes the IP address and port of the URL or endpoint. If their devices support auto-enrollment to a public URL, auto-enrollment is available as part of the tenant, and configuration details are provided in the documentation.

The cloud connector is advised for DMZ-based deployments or for enrollment through your cloud connector. This is especially useful in scenarios where endpoints cannot communicate with a public URL for auto-enrollment through a private channel, necessitating the use of the cloud connector.

- EST
- ACME
- SCEP
- MS Intune
- CMP
- WAEP
- Actions
- Direct Requests

EST

EST stands for Enrollment over Secure Transport. It is a certificate management protocol targeting Public Key Infrastructure (PKI) clients which require digital certificates to prove their authenticity. EST also helps the clients in acquiring associated CA certificates. Some prerequisites and features are as follows:

- There should be an agent (avx_vendor_cert_est_agent) up and running for EST in AppViewX.
- This EST plugin can either be in HTTPS or HTTP, but it needs a gateway which supports client certificate authentication running to communicate with the client.
- It is highly recommended to keep the 'Approval Required' flag OFF in the **Menu > Inventory > Certificate > Policy** page.
- The valid agent setting should be available in **Menu > Inventory > Certificate > Settings**.

The Enrollment over Secure Transport protocol or EST is a certificate management protocol that automates the issuance and provisioning of X.509 certificates. The protocol has been defined in RFC 7030 (ratified in 2013) and developed for clients that use public key infrastructure (PKI), such as web servers, applications, and endpoint devices.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The protocol helps configure PKI clients to request for certificates from trusted certificate authorities (CAs) and receive them over secure HTTPS without any human intervention.

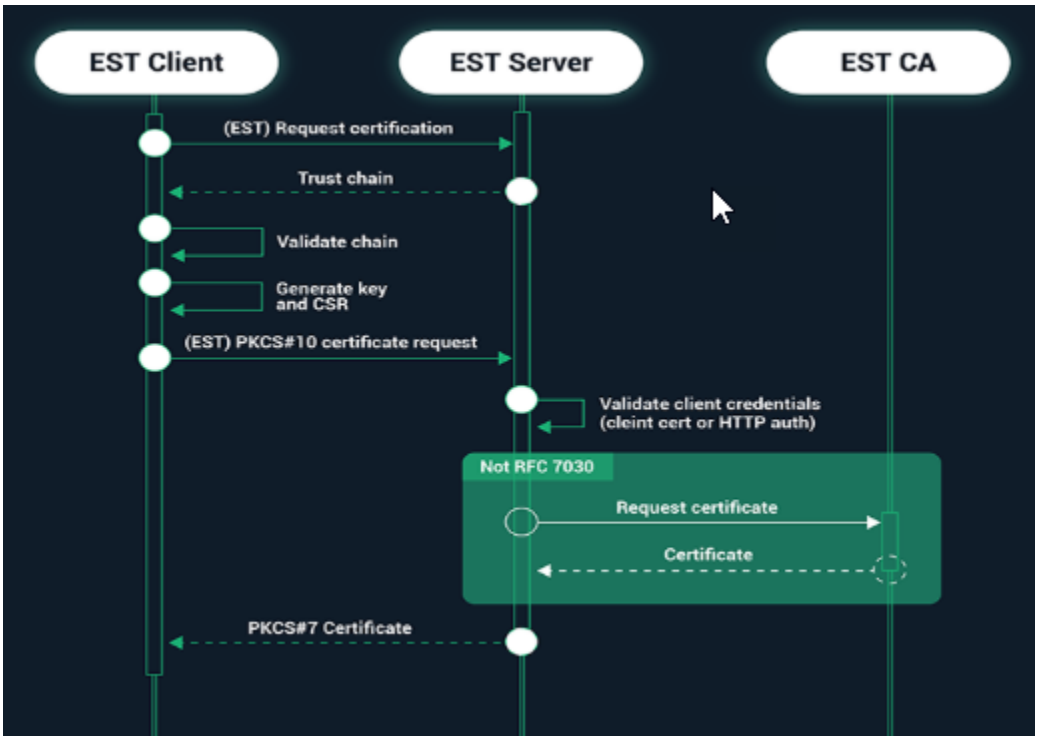
- Configuring AppViewX EST Server
- Configuring AppViewX EST Client
- EST Micro CA (Standalone Server)

What is the Purpose of EST?

The main goal of EST is to simplify and secure certificate enrollment. EST helps ensure certificates are correctly configured and deployed at scale by automating the process. Removing human intervention naturally reduces the risk of misconfigurations, and, in turn, the reduces the possibility of outages and security compromises. Automating enrollment also helps free up time for PKI personnel who are otherwise caught up in the perpetuity of getting certificates issued and provisioning them.

How does EST work?

In an enterprise PKI setup, the EST server sits between a client and a certificate authority (CA) and plays the role of a traditional Registration Authority (RA) – receive a certificate signing request (CSR) from a client, validate the client, forward the request to the corresponding CA, get the certificate issued, and finally provision it to the client.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The EST communication between a client and a certificate authority happens as follows:

1. The client hits the server with a request to communicate over TLS. The server responds to the request by presenting its TLS certificate.
2. The client checks the certificate to verify the legitimacy of the server. Next, it requests the chain of trust from the server and verifies it, including any intermediate certificates that lie between the root and the EST CA, and stores the root certificate.
3. The client generates a key and a CSR and sends the CSR to the server.
4. The EST server forwards the CSR to the CA and receives a new certificate. It then sends the newly signed certificate back to the client.

Advantages of using EST

EST is an auto-enrollment protocol that offers various functionalities such as enrollment, re-enrollment, and server-side key generation. This protocol serves as the foundation for the client and ensures interoperability with other EST-compliant servers.

What's Next?

Configuring AppViewX EST Server

Prerequisites

On-prem

- Make sure that the following pods are running in the cluster by using the command:

```
kubectl get pods -A | grep est
```

```
ppviewx@pm-saas-node33:~$ kubectl get pods -A | grep est
bsecon                avx-vendor-cert-est-agent-549985fbfc-kwzjm                3/3     Running     0               8d
ppviewx@pm-saas-node33:~$
```

- Make sure that <avx-platform-gateway-est> and <avx-vendor-cert-est-agent> services are running in the cluster by running:

```
kubectl get svc -A | grep est
```

```
appviewx@pm-saas-node33:~$ kubectl get svc -A | grep est
absecon               avx-vendor-cert-est-agent             ClusterIP   10.102.47.223   <none>        5306/TCP
external-system       avx-platform-gateway-est              NodePort    10.97.224.10    <none>        5301:3002
```

SaaS

Ensure the https gateway is enabled on the cloud connector while installing it. To do this:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Navigate to the installation directory of the cloud connector software.
2. Run

```
cd deps/tools
```

3. Run

```
./k3s kubectl get svc -A | grep mtls
```

Note: It should have the avx-mid-server-gateway-mtls under namespace cc.

```
[appviewx@pe-qa-cc-n8 tools]$ ./k3s kubectl get svc -A | grep mtls
cc            avx-mid-server-gateway-mtls    NodePort    10.43.0.141   <none>        5301:30021/TCP          22h
[appviewx@pe-qa-cc-n8 tools]$
```

Enabling EST Services

For On-prem

1. Log onto the AppViewX installer node.
2. Go to </installation_folder/appviewx_kubernetes/scripts> folder.
3. Add the avx-vendor-cert-est-agent and avx_platform_gateway_external in ENABLED_PLUGINS in the appviewx.conf file.
4. Specify the datacenter (DC) where the gateway must be deployed:
   - avx_vendor_cert_est_agent=<dc name>
   - avx_platform_gateway_external=<dc name>

```
ENABLED_PLUGINS=appviewx_dependencies,avx_commons,avx_crontab,avx_config_server,avx_platform_core,avx_platform_amc,avx_platform_q
ueue,avx_platform_gateway,avx_platform_gateway_external,avx_platform_web,avx_subsystems,avx_vendors,avx_subsystems_sync,avx_visua
l_page_builder,avx_vendor_cert_network_discovery,avx_vendor_cert_scep_agent,avx_vendor_cert_intune_agent,avx_vendor_cert_est_agen
t,avx_vendor_cert_acme_agent
SSH_OTHER_USER=appviewx

avx_commons=absecon
avx_config_server=absecon
avx_platform_core=absecon
avx_platform_queue=absecon
avx_subsystems=absecon
avx_subsystems_sync=absecon
avx_vendors=absecon
avx_platform_gateway=absecon
avx_platform_web=absecon
avx_platform_amc=absecon
avx_platform_gateway_external=absecon
avx_visual_page_builder=absecon
avx_vendor_cert_network_discovery=absecon
avx_vendor_cert_scep_agent=absecon
avx_vendor_cert_intune_agent=absecon
avx_vendor_cert_est_agent=absecon
avx_vendor_cert_acme_agent=absecon
```

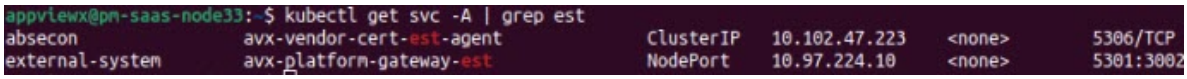
5. Run <plugins_install.sh>
6. Verify if EST is enabled by running kubectl get pods -A | grep est

```
ppviewx@pm-saas-node33:~$ kubectl get pods -A | grep est
bsecon          avx-vendor-cert-est-agent-549985fbfc-kwzjm              3/3     Running     0              8d
ppviewx@pm-saas-node33:~$
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Verify the plugin status and port number:
   a. Make sure that avx-vendor-cert-est-agent and avx-vendor-cert-est-agent are running by using the command:

```
kubectl get services -A | grep est
```



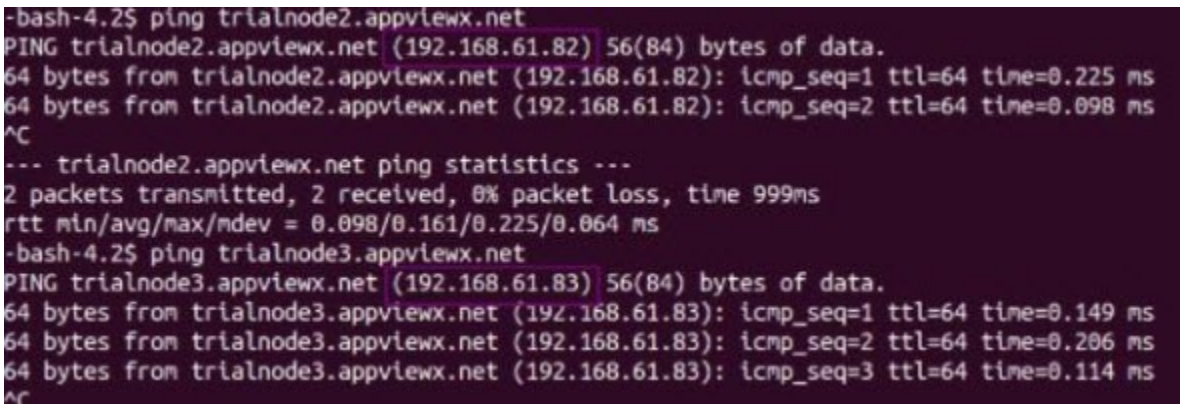
   b. Make sure that the port number is 5301:30021 in avx-platform-gateway-est.

> **Note:** The number 30021 must be used in the UI configuration.

   c. Identify the nodes running the EST service. EST is available on all the nodes where the external system runs by running:

```
<kubectl get pods -n external-system -o wide>
```

   d. Ping to the node names to fetch the IP addresses.



For SaaS

HTTPS gateway must be enabled while installing the cloud connector (CC). To do this:

1. Log onto the cloud connector installed node.
2. Go to cc_installed_path/deps/properties.
3. Open appviewx.properties and set the following fields as *true:*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. AUTO_ENROLL_ENABLED=true
b. ENABLE_MTLS_PROFILE=true
c. ENABLE_HTTP_PROFILE=true
d. ENABLE_HTTPS_PROFILE=true

4. Scale down the avx-mid-server-platform pod.
5. Restart the avx-mid-server-starter pod.

> **Note:** Ensure that avx-mid-server-gateway-https is present under namespace cc.

Configuring EST Server

1. Go to **(Menu)** > **CERT+** .
   The left navigation pane appears.
2. Select **Administration** > **Auto Enrollment** > **EST**.
3. Click **+ Add** icon on the top-right.
   The **Auto Enrollment : EST** page is displayed.
4. Enter the following details:

Endpoint Details - Field Description Table

Fields	Description
Endpoint Details	
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	**For On-prem** • **Without load balancer:** Must contain the FQDN of the node where the external gateway is running. To get the details, run `kubectl get pods -n external-system -o wide`. If the external gateway is running on multiple nodes, you can specify any one of those nodes. • **With load balancer:** Must be the FQDN of the load balancer. **For SaaS:**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Using On-premises CC: • **Without load balancer:** Must be the FQDN of the cloud connector where the auto-enrollment gateway is running. • **With load balancer:** Must be the FQDN of the load balancer. **Using Direct Gateway** In the SaaS setup, to use the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***Port**	**For On-prem** • **Without load balancer:** By default, it is port 30021. Leave it as is. • **With load balancer:** Port must be the listening port of the load balancer. **Note:** • It is recommended to set the listening port as 30021, which is the same as AppViewX. • If the load balancer's listening port is different from 30021, then update the respective port. **For SaaS:** **Using On-premises CC:** • **Without load balancer:** By default, it is port 30021. Leave it as is. • **With load balancer:** Port must be the listening port of the load balancer. **Note:** • It is recommended to set the listening port as 30021, which is the same as AppViewX. • If the load balancer's listening port is different from 30021, then update the respective port. **Using Direct Gateway**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only port 443.
Client Authentication	
Authentication Mode	Select any one authentication method to be carried out during communication with clients: • **Only Certificate TLS:** During client authentication, only certificate TLS based authentication will be performed. • **Certificate TLS with HTTPS fallback:** During client authentication, when the certificate TLS fails, HTTPs based authentication is performed as fallback. • **Both Certificate TLS and HTTPs:** During client authentication, both certificate TLS and HTTPs authentication are performed one after the successful completion of the other. **Using Direct Gateway** In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use only **Certificate TLS with HTTPS fallback** as the Authentication mode.
***Issuer Certificate**	Select one or more issuer certificates that need to be checked for the client certificate authentication.
***Client Certificate Revocation Check**	By default, the value is set to **No Revocation Check.** Choose from any of these values: • **No Revocation Check:** Client certificates will not be checked for revocation. • **Perform Revocation Check:** Certificates will be validated against revocation mechanisms using CRL or OCSP. • **Check Inventory for Revocation:** Certificates will be checked against the certificate inventory for revocation status.
***HTTP Authentication Mode**	This field appears when Authentication Mode = Certificate TLS with HTTPS fallback or Both Certificate TLS and HTTPs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Select the type of HTTP auth mode either Basic/Digest. • **Basic:** During client authentication, only the username and password values are considered for HTTPs based authentication. • **Digest:** During client authentication, nonce and realm values are also supported along with username and password.
***Fallback Credentials**	This field appears when Authentication Mode = Certificate TLS with HTTPS fallback or Both Certificate TLS and HTTPs. Select Manual/Logged on user credentials - based on the selection users can configure the credentials manually or save as credentials equivalent to the logged in user. • **Manual:** The Username and Password fields will be displayed to enter values. • **Logged on user credentials:** The Username and Password fields will not be displayed.
***Username**	Enter username for HTTP authentication.
***Password**	This field appears when Authentication Mode = Certificate TLS with HTTPS fallback or Both Certificate TLS and HTTPs. Enter password for HTTP authentication.
CA Accounts	
***Certificate Group**	Select a specific group under which certificate needs to be enrolled.
***Certificate Category**	Select a specific certificate type (Server / Client / Intermediate) to be enrolled. **Note:** The intermediate radio button, filters templates to show only SUB-CA templates suitable for intermediate CA issuance designed for the microCA functionality.
***Select CA**	Select the required CA from the available options. The certificate is enrolled under the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS • AppViewX PKIaaS Native • Amazon Private CA • DigiCert • DigiCert One • EJBCA • Entrust • Entrust MPKI • GlobalSign Atlas • GlobalSign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust • Sectigo (Comodo Certificate Manager) • SwissSign
***: Mandatory fields	

Load Balancer Configuration

It is recommended to set the listening port as 30021, which is the same as AppViewX.

Health check URL for load balancer:

a. **HTTP method:** GET
b. **Healthcheck API:** https://<hostname>:30021/
   i. **FQDN:** FQDN of cloud connector enabled with the MTLS gateway.
   ii. **Expected response code:** 401. As the load balancer is accessing the URL without any parameters, it will receive a 401 response.

The load balancer needs to be configured to forward client certificates (used for MTLS authentication) to AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA configuration

When **AppViewX** is selected as CA, the fields for AppViewX CA are as follows:

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. **Note:** For some CAs, the validity available in their respective CA portal is considered despite the specified certificate validity.
*: Mandatory fields	

When **AppViewX PKIaaS Native** is selected as CA, the fields for AppViewX PKIaaS Native CA are as follows:

Details for AppViewX PKIaaS Native - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Template Name	Select a template name from the dropdown list.
***Issuer Name**	Select an issuer name to issue the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. **Note:** For some CAs, the validity available in their respective CA portal is considered despite the specified certificate validity.
*: Mandatory fields	

When **Amazon Private CA** is selected as CA. The fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the group's associated policy. Select an appropriate value as required.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Order Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

When **AppViewX PKIaaS** is selected as CA. The fields for AppViewX PKIaaS CA are as follows:

Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***Issuer Location**	Select the issuer location associated with the CA account.
***Issuer Name**	Select a valid issuer associated with the CA account.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

When **DigiCert** is selected as CA. The fields for DigiCert CA are as follows:

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Division**	Select a division associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	Select a valid certificate type associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Order Validity**	Validity of the certificate to be enrolled.
*****: Mandatory fields	

If the **Select CA = DigiCert**, then a separate section **Vendor Specific Details** is displayed after the CA Accounts section with two fields described below.

Vendor Specific Details for Digicert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type. The dropdown is populated with the first available value. Select an appropriate value as required.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with the account balance. Returns an error if this option is disabled for the account or if the account has an insufficient fund. • **Bill To Default Credit Card** - Pay with the account's default credit card. Returns an error if no default credit card is configured for the account
*****: Mandatory fields	

When **DigiCert One** is selected as CA. The fields for DigiCert One CA are as follows:

Details for DigiCert One CA - Field Description Table

Fields	Description
***CA Account Name**	A unique name to identify the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server or Client.
Proxy Required	Enable this field if the CA communication needs to happen via proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center for CA communication, with the CC node being the recommended option. The selected node will handle the communication through the chosen CC node.
CA Configuration	
***Base URL**	This URL will contain the hostname of the DigiCert CA instance and used for constructing the API requests.
***Authentication method**	By default, API Token is selected.
***API Token**	Enter the API token to authorize the communication between AppViewX and DigiCert One.
Allow Seat ID during enrollment	Enabling this field displays a Seat ID field in the Auto enrollment settings that you can use instead of the CA settings.
***Seat ID**	Unique value assigned to identify an entity in the DigiCert One account.You can provide multiple ID separated by a comma. They can be used for enrollment, renewal, and regeneration.
Use DigiCert One to switch certificates from DigiCert MPKI	Enable this field to automatically switch your DigiCert MPKI certificates to DigiCert One with auto-enrollment/auto-regenerate.
*: Mandatory fields	

When **EJBCA** is selected as CA. The fields for EJBCA CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
*: Mandatory fields	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
*: Mandatory fields	

When **Entrust** is selected as CA. The fields for Entrust CA are as follows:

Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	Select a valid certificate type associated with the CA account. • If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. • If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: Mandatory fields	

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the requester name.
Requester Email	Enter a valid email ID.
Requester Phone	Enter the 10-digit phone number.
*: Mandatory fields	

When **Entrust MPKI** is selected as CA. The fields for Entrust MPKI CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: Mandatory fields	

If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Certificate Profile**	Select a certificate profile from the dropdown list.
*: Mandatory fields	

When **GlobalSign Atlas** is selected as CA. The fields for GlobalSign Atlas CA are as follows:

Details for GlobalSign Atlas CA - Field Description Table

Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***API Credential Friendly name**	Select a CA Account to communicate with during the certificate enrollment actions.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
***: Mandatory fields	

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.

When **GlobalSignMSSL** is selected as CA. The fields for GlobalSign MSSL CA are as follows:

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Product Type**	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled (in days/months/years).
***: Mandatory fields	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile name**	Select the Profile based on the configurations made in the Certificate Authority setting.
***: Mandatory fields	

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
*: Mandatory fields	

When **Google** is selected as CA. The fields for Google CA are as follows:

Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
Template Name	Select the appropriate template name.
***Issuer Name**	Select an issuer name to issue the certificate.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

When **HydrantID** is selected as CA. The fields for HydrantID CA are as follows:

Details for HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

When **IDnomic** is selected as CA. The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: Mandatory fields	

When **Microsoft Enterprise** is selected as CA. The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: Mandatory fields	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed with a **Template Name** dropdown after the CA Accounts section.

When **Microsoft Standalone** is selected as CA. The fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: Mandatory fields	

When **Nexus** is selected as CA. The fields for Nexus CA are as follows:

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: Mandatory fields	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor Specific Details - Field Description Table

Fields	Description
***Procedure**	Select the procedure based on the configurations made in the Certificate Authority Setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: Mandatory fields	

When **OpenTrust** is selected as CA. The fields for OpenTrust CA are as follows:

Details for OpenTrust CA - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Certificate Management Profile**	Select the certificate issuance policy defined in OpenTrust CA.
Zone	The AppViewX configuration wrapper that maps to a CA + profile, and is used by end-users or automation to request certificates consistently.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: Mandatory fields	

A **Profile Parameters** section is also displayed below the CA Accounts section. It contains the fields such as **Common Name*, *Organizational Unit*, **Organization*, **Email*, **Password*. or as configure in the Certificate Authority settings page.

When **Sectigo (Comodo Certificate Manager)** is selected as CA. The fields for Sectigo (Comodo Certificate Manager) CA are as follows:

Details for Sectigo (Comodo Certificate Manager) CA - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Certificate Type**	Certificate Type for which CLM actions will be enabled.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: Mandatory fields	

When **SwissSign** is selected as CA. The fields for SwissSign CA are as follows:

Details for SwissSign CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate creation operations.
***Client Name**	Select the specific client.
***Product**	Select the specific product.
***CA Certificate**	Select the specific issuer certificate that will be used for signing CSR by the certificate authority. Certificates available in the root or intermediate certificate inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

5. Configure the **Advanced Settings** details as follows:

   The following table provides the field description for Advanced Settings:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Advanced Settings - Field Description Table

Fields	Description
***Switch to Enroll**	Select *Yes* or *No*. Selecting the radio button as *Yes* will convert the re-enrollment requests to enrollment requests.
***Fetch Certificate Parameters**	Select *Yes* or *No*. Setting the radio button to *Yes* will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.
***Include Truststore Certificates**	Select whether the issuer certificate needs to be sent to client machines after enrollment.
***High Speed Transactions**	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. Request information pertaining to High-Performance can be viewed on the Direct Requests page.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed. • If the option is disabled (**No**), then AppViewX will do the default behavior of enrolling a new certificate for each request.
Certificate Threshold	This field is enabled only if **Return Existing Certificate = Yes.** Enter the number of days in this field. This value is used to Initiate a new certificate request if the certificate is nearing the expiry date i.e., if existing certificate validity is less than the entered value.
***Retry Count**	Values accepted between 5 - 99.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received.
***Retry Frequency**	Values accepted between 10 - 99. The value specified in this field determines the duration taken between the trigger calls by the EST agent.
*: Mandatory fields	

Iptables and Pod Scaling in Worker Nodes

As part of the **CIS benchmark compliance** for AppViewX on-prem servers, only the **default ports** are whitelisted by default. Any additional ports—such as **30021** or **30022** required for **Auto Enrollment Protocol** operations—must be explicitly allowed in the **iptables** configuration.

In this case, **port 30021 (EST)** is an additional plugin port that must be permitted in the iptables rules to enable external communication.

Follow these steps to add the required rule to the iptables configuration:

1. Connect to the worker nodes:

   `vi /etc/iptables/rules.v4`

2. Add lines to the IPtables to ACCEPT traffic30021, 30022:

   `iptables-restore < /etc/iptables/rules.v4`

3. To scale the pods on a worker node:

   `kubectl scale --replicas=2 deploy/avx-platform-gateway -n external-system`

To include the iptables rules:

1. Open the rules.v4 file:

   `sudo -i`

   `vi /etc/iptables/rules.v4`

2. Append the following lines to allow the required ports:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
-A INPUT -p tcp -m tcp --dport <port> -j ACCEPT
```

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 31443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 30021 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 30022 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 30190 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 179 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 6443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 10250 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 2379 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 2380 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 9100 -j ACCEPT
-A INPUT -p udp -m udp --dport 4789 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW -j ACCEPT
-A INPUT -p icmp --icmp-type timestamp-request -j DROP
-A OUTPUT -p tcp -m tcp --sport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
COMMIT
```

Here, we have added 30021 and 30022 ports.

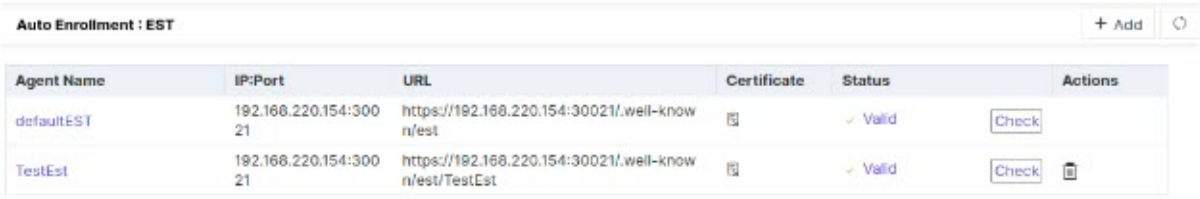
3. Save and apply the rules:

```
iptables-restore < /etc/iptables/rules.v4
```

Verifying EST Server

To validate the AppViewX configuration:

1. The agent configuration must be in **valid** status.



2. If the configuration is completed and agent status is valid, refresh the EST URL from the web browser. The expected response must be:

```
{"appStatusCode":"AVX_GW_021","message":"Client certificate authentication failed"}
```

As no client certificate is provided when entering this URL, there will be a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Operations

The AppViewX EST agent supports these operations:

Supported Operation	Operation Path
Distribution of CA certificates	/cacerts
Enrollment of clients	/simpleenroll
Re-enrollment of clients	/simplereenroll

Actions using EST Server

You will be prompted with the question, *Do you want to bind a SSL certificate to gateway? (y/n)*:

a. To bind a certificate to the gateway, enter **y**.

b. You will then be asked for the *certificate path* and the *key path*. Provide the relative path of the files as indicated:

If the certificate and key file is copied into <cc_installation_folder>/deps/properties/ folder, then the path should be:

- *Please enter the certificate file path:* /properties/test.crt
- *Please enter the key file path:* /properties/test.key

c. If this step is not required, enter **n**.

Enrolling Server Certificate

If you do not have a client-authentication AppViewX CA certificate, you can use AppViewX CA.

Note: When the database flag CERT_AUTO_ENROLLMENT_ENABLE_REENROLL is enabled, AppViewX can detect previously enrolled certificates. If it finds certificates with the same Common Name (CN) from the same device, it will treat them as re-enrollment and preserve their history. Otherwise, it will proceed with the standard enrollment process. This ensures that certificate history is maintained, even after the EST client is reinstalled.

To use a client-authentication AppViewX CA certificate:

1. Log on to the AppViewX application with valid credentials.
2. Go to **(Menu)** > **CERT+** .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Select **Certificate Action > Enroll Certificate > Server**.
   The **Enroll Server Certificate** page appears.
4. In the **General Information** section of the **Enroll Server Certificate** page, select the desired **Assign Group** from the dropdown list. By default, the **Default** option is selected.
5. Enter the **CA Details**.

Field descriptions for the CA Details section

Fields	Description
***Certificate Authority**	From the dropdown list, select the CA.
***Renew Automatically**	**Note:** Changing the group inherited renew period overwrites the renewal period for this certificate. Select the toggle button to On or Off. • When the toggle is enabled, the Start Renewing option is enabled. • Enter the number of days to renew the certificate automatically.
***Regenerate Automatically**	Select the toggle button to On or Off. • When the toggle is enabled, the Start Regenerating option is enabled. • Enter the number of days to renew the certificate automatically.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request is submitted.
Certificate Profile	From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	This field is displayed when **Certificate Authority** = **IDnomic** and a CA+RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that is used for certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Connector Name**	Enter the friendly name for the CA connector. On saving this form, the name entered here is displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>From the following options, select the required method for generating the CSR:
• AppViewX: Private key and CSR are created in AppViewX based on CSR parameters given.
• Upload CSR: You can upload a file that contains the CSR details. This source file is used to populate the CSR parameters, which is submitted to the CA.
a. Under CSR Generation, select Upload CSR.
The Please paste your CSR field is displayed.
b. From the Please paste your CSR field, select Browse.
c. Navigate to the location of your CSR file, and click Open.
d. Click Upload.
• HSM:
Note: This option is disabled when Certificate Authority = Google.
To generate the private key and the CSR, based on the CSR parameters given, in an HSM device:
a. Under CSR Generation, select HSM.
b. Fields for gathering your HSM-related inputs are displayed.
To generate the private key and the CSR, enter/select the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>From the dropdown list, from the following options, select the type of device on which the private key and the CSR are generated:
• HSM Devices
• ADC Devices</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Vendors</td><td>This field is applicable only when Device Type = ADC Devices.</td></tr>
<tr><td>*Devices</td><td>This field is populated based on the Device Type and Vendors selected.

From the dropdown list, select the required HSM/ ADC device.</td></tr>
<tr><td>*Key Handler Name</td><td>This field is applicable only when Device Type = HSM Devices.Enter the key handler name.</td></tr>
<tr><td>*Key Reference Name</td><td>This field is applicable only when Device Type = ADC Devices. Enter the key reference name.</td></tr>
</table>
• End Point:

Note: This option is disabled when Certificate Authority = Google.
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>To generate the private key and the CSR in the selected end point device, enter/select the following inputs:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>From the following options, select the ADC device category:
• ADC
• Server
• Firewall</td></tr>
<tr><td>Vendor</td><td>From the dropdown list, select the vendor of the end point device.

Note: This field is populated based on the Category selected.</td></tr>
<tr><td>*Devices</td><td>This field lists the end point devices present in your environment that belong to the above selected Category and Vendor.

From the dropdown list, select the end point device on which you want to generate the private key and the CSR.</td></tr>
<tr><td>Tenant</td><td>This field is applicable only when Category = ADC. Enter the tenant ID.</td></tr>
</table></td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description

Field	Description
CSR Location	This field is applicable only when **Category** = **Server**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. As the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, this field is labeled as **CSR File Location** for enrolling Apache server certificates.
***Key File Name**	Enter the name of the file that contains the private key details. As the extension is already included in the field, ensure

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>that you enter the file name without the file extension.

Note: Starting from v2023.1.0 FP2, this field is labeled as Key File Location for enrolling Apache server certificates.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

6. For the certificate being enrolled, enter the **CSR Parameters**.

Field descriptions for the CSR Parameters

Field	Description
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note:** No special characters allowed except underscore (_) and hyphen (-).
Subject Alternative Name	Enter/From the dropdown list, select the Subject Alternative Name for the certificate being enrolled. You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Multiple values must be separated by a comma. • The cumulative count of SANs is displayed in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field is auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field is auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field is auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field is auto-filled and editable based on the configuration in the selected group's policy.
Country	Country name is one of the CSR parameters to be present in the certificate. This field is auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	Enter a valid email address of the person responsible for maintaining the certificate.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password from the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field is auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field is auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field is auto-filled and editable based on the configuration in the selected group's policy.
***: Mandatory fields	

7. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used only for reference.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
***: Mandatory fields	

8. In the **testAttributelabelTest** field of the **Certificate Attributes** section, enter the organization-specific values that need to be mentioned along with the CSR.
   These values are not part of the certificate but are available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

9. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow.
First name	This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. First name (as a metadata) associated with the certificate to be enrolled.
Last name	This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Last name (as a metadata) associated with the certificate to be enrolled.
Organization	This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Organization name (as a metadata) associated with the certificate to be enrolled.
Comment	This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Additional information (as a metadata) associated with the certificate to be enrolled.
UUID	This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled.

10. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters for their operational purposes.
    - By default, the **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section).
    - The **Certificate ID** can be modified by the user.
    - If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**.
    - If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.
11. Click **Add**.
    Once the details are added, you are redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
12. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
13. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
14. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
15. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

16. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
17. Click **Implement**.
    The **Implement** dialog box is displayed.
18. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
19. Click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CSR Submission to CA is in progress. Once the CSR submission is successful, the request state changes to **Submit** certificate - retrieval in progress state.

If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate is fetched in a few seconds.

If auto-approval disabled in the targeted CA, you have to be logged into the CA and approve the request.

Once the certificate is issued successfully, the certificate is retrieved into AppViewX.

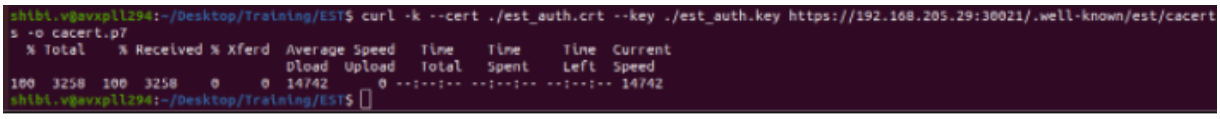
Testing EST Enrollment

To test the EST enrollment:

1. After successful verification, create a test folder in the Linux client machine.
2. Download the client authentication certificate (est_auth.crt) and the key (est_auth.key).

> **Note:** The common name of the client authentication certificate can be any value, but the file name of the client certificate to be used in EST client must be est_auth.crt and est_auth.key.

3. Trigger the GetCA certificates request using the curl command.
4. Make sure that the authentication certificate and the key are present in the same location: <curl -k --cert ./est_auth.crt --key ./est_auth.key<EST Endpoint URL from AppViewx GUI>/cacerts -o cacert.p7>.



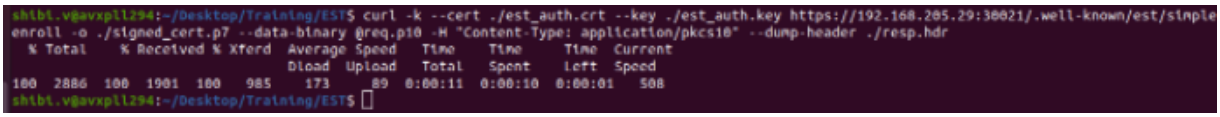
You will get the <cacert.p7> file with the enrolled CA certificate in Step 9.

5. Convert the received CA certificate to pem:

```
openssl base64 -d -in cacert.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out cacert.pem>
```

6. Trigger the enrollment request by using the curl command. Make sure that the authentication certificate, key, and CSR are present in the same location.

```
curl -kv --cert ./est_auth.crt --key ./est_auth.key <EST Endpoint URL from AppViewx GUI>/simpleenroll -o ./signed_cert.p7 --data-binary @req.p10 -H

"Content-Type: application/pkcs10" --dump-header ./resp.hdr
```



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. Verify the content of <signed_cert.p7>.

8. Convert the enrolled p7 certificate into pem:

```
<openssl base64 -d -in signed_cert.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out signed_cert.pem>
```

9. Make sure that you received the <cacert.p7> file with the enrolled CA certificate.

[Optional] Adding External CA Trust Certificate for EST Client Authentication

On-prem

1. By default, the AppViewX intermediate and the AppViewX root certificates are available in the location with filenames default_inter.crt and default_root.crt.
2. Run:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
[appviewx@pesrv07-arch-94-20 ~]$ kubectl describe secret client-cacerts-est -n external-system
Name:         client-cacerts-est
Namespace:    external-system
Labels:       <none>
Annotations:
Type:         Opaque

Data
====
default_inter.crt:  1505 bytes
default_root.crt:   1281 bytes
[appviewx@pesrv07-arch-94-20 ~]$
```

3. Download the required issuer certificates in .crt format and move them to the AppViewX installer node.
4. Open appviewx.conf file in appviewx_kubernetes/scripts folder.
5. Add the absolute path of the issuer certificates as key separated value in EST_TRUSTED_CA_CERTS.

```
# Comma seperated values of absolute paths of certs
EST_TRUSTED_CA_CERTS=/home/appviewx/certs/digicert_issuer.crt
```

6. Add these plugins in the ENABLED_PLUGINS list:
   ENABLED_PLUGINS=appviewx_dependencies,avx_platform_gateway_external,avx_platform_gateway
7. Run `./plugins_install.sh`

SaaS

EST Client Authentication in Cloud Connectors

This section describes the steps to replace the Default TLS Certificate with Signed Certificate and to add a CA issuer certificate for EST client authentication in CC (Cloud Connector).

By default, AppViewX provides a default certificate in the gateway. To enable TLS validation youvalidationFor ACME you must bind a valid certificate (Certificate with CC hostname) with the gateway.

[Optional for EST] To bind a TLS certificate to gateway:

- The certificate's common name must be the hostname of the CC.
- Download the certificate with .crt format and key file.

Note: By default, AppViewX cloud connector allows only the AppViewX CA issued certificates for client authentication. To add other CA issuer certificates for EST client authentication, download the required issuer certificates in .crt format.

To update the certificate:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Copy the certificate and the key file to <cc_installation_folder>/deps/properties/ directory.
2. Go to the cc_installation_folder and run:

```
./avxctl upgrade gateway-cert
```

3. You will be prompted with the question, *Do you want to bind a SSL certificate to gateway? (y/n)*:
   a. To bind a certificate to the gateway, enter **y**.
   b. You will then be asked for the *certificate path* and the *key path*. Provide the relative path of the files as indicated:

      If the certificate and key file is copied into <cc_installation_folder>/deps/properties/ folder, then the path should be:

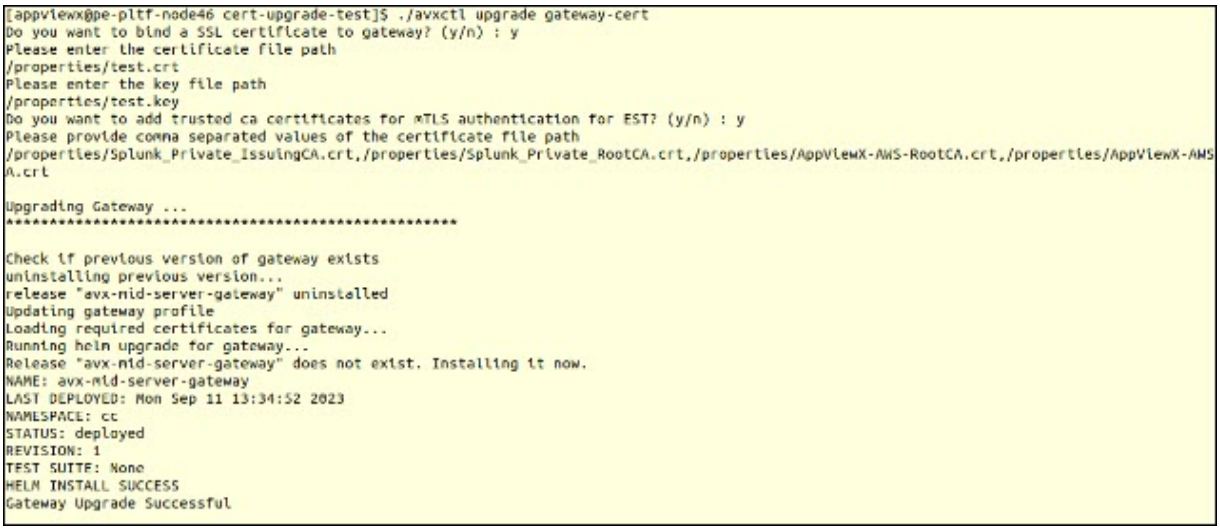
      • *Please enter the certificate file path:* /properties/test.crt
      • *Please enter the key file path:* /properties/test.key

   c. If this step is not required, enter **n**.
4. You will now be prompted with, *Do you want to add trusted CA certificates for mTLS authentication for EST? (y/n):*
   a. To give the issuer certificate list of the client certificate used in EST enter **y**.
   b. You will then be asked for the *certificate path*. You may give more than one certificate path using a comma (,).

      If the issuer certificates are copied to <cc_installation_folder>/deps/properties/ folder, then the path should be:

      Please provide comma separated values of the certificate file path: /properties/test.crt

   c. If this step is not required, enter **n**.
5. Wait for the script to complete and the gateway will be upgraded.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

[Optional] Changing SSL Certificate for EST-HTTPS Communication

Note: This section is applicable only for on-premise installation.

- By default, there is a self-signed certificate available in the location.
- Add the following plugins in the ENABLED_PLUGINS list:

ENABLED_PLUGINS=appviewx_dependencies,avx_platform_gateway_external,avx_platform_gateway

```
# Please specify the absolute paths of files for the labels below
# EST_SERVER_ACCESS_CERT=
# EST_SERVER_ACCESS_KEY=
# Comma seperated values of absolute paths of certs
#EST_TRUSTED_CA_CERTS=/home/appviewx/appviewx_kubernetes/scripts/digicert.crt
```

- Run `./plugins_install.sh`

```
[appviewx@pesrv07-arch-94-20 ~]$ kubectl describe secret server-tls-est -n external-system
Name:         server-tls-est
Namespace:    external-system
Labels:       <none>
Annotations:
Type:         kubernetes.io/tls

Data
====
tls.crt:  1046 bytes
tls.key:  1704 bytes
```

Best Practices

- **Certificate Group and CA Policy Setup:**
  - Create a dedicated certificate group and CA policy specifically for auto-enrollment in AppViewX.
  - While configuring the policy, ensure only the required key bit-length is selected (minimum: **2048-bit**).
- **Machine Enrollment Controls:** Define an expected domain pattern (e.g., *.appviewx.com) in the CA policy to restrict certificate issuance to authorized machine domains.
- **Security Recommendations:**
  - **TLS Authentication** is strongly recommended for all EST client communications with AppViewX.
  - Use only **private/internal CAs** as trusted issuers for client certificate authentication.
  - If client certificates from non-AppViewX CAs are used, ensure the **Intermediate and Root CA certificates** are properly bound to:
    - The AppViewX **external gateway** (for on-prem deployments)
    - The AppViewX **mid-server gateway** (in Cloud Connector for SaaS deployments)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Certificate Type Selection:** Choose the correct certificate category: **Server** category for server certificates only, and **Client** category for machine and user certificates
- **High Availability and Load Balancing:** When multiple external gateways (on-prem) or Cloud Connectors (SaaS) are in use, it is recommended to deploy a **Load Balancer with mTLS**. This ensures secure and reliable EST client authentication using the certificate and key-based requests.

Example of URLs

- For default: `<https://est.appviewx.com:<port_number>/.well-known/est>`
- For AppViewX enrollment: `<https://est.appviewx.com:<port_number/.well-known/est/appviewx/simpleenroll>`
- For AppViewX re-enrollment:

```
<https://est.appviewx.com:<port_number/.well-
known/est/appviewx/simplereenroll>
```

Configuring AppViewX EST Client

- EST Client v1.5.4

Prerequisites

- Configure EST server in AppViewX.
- Administrator access is required to run AppViewX EST client 1.5.0.
- Ensure that the firewall configuration permits communication from the EST client. (Port 30021 for both on-prem and SaaS setup.)
- If a load balancer is part of the network infrastructure for the endpoint to communicate with the EST agent, make sure the load balancer does not terminate the client authentication certificate. If it does terminate, then configure the EST authentication mode as **Certificate TLS with HTTP as a fallback** in the EST endpoint configuration in AppViewX.

System Requirements

Linux

Operating System: The supported operating system and their versions are mentioned as follows:

Operating System	Version
Red Hat	v8.6 and later
Ubuntu	v20.04 and later

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operating System	Version
CentOS	v7.9 and later
Debian	v11.0 and later
Mint	v18.2 and later
openSUSE	v15.0 and later

Mac

Operating System	Version
Sonoma	v14.0 and later
Ventura	v13.0 and later

Windows

Operating System: Windows v7.0 and later

Installing EST Client

This section provides instructions on how to install and configure the AppViewX EST client agent on Linux, Windows, and Mac machines. The installation and configuration process follow these steps:

1. Downloading and extracting the EST client on Linux and Mac machines and Windows machine.
2. Configuring the EST client.
3. Running Generator and Installer EST client on Linux and Mac machines and Windows machine.

On Linux and Mac

1. Log on to the AppViewX release portal.
2. Download:
   - **For Linux:** est-client-linux-1.X.0.zip
   - **For Mac:** est-client-mac-1.X.0.zip
3. Extract the above zip file to the desired file location.

   The extracted file contains two subfolders:
   - appviewx_est_client_installer
   - appviewx_est_client_installer_generator

   In the appviewx_est_client_installer folder are:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- input
  - **Linux:** contains appviewx_client, config.json, DATA
  - **Mac:** contains appviewx_client, appviewx_client.app, config.json
- • **Linux:** appviewx_est_client_installer
  - **Mac:** appviewx_est_client_installer.app
- current_crontab.txt (present only for Linux)
- README.md
- uninstall.sh

In the appviewx_est_client_installer_generator folder are:

- input (contains credentials, est_auth.crt, est_auth.key, secure_config.json)
- • **Linux:** appviewx_est_client_installer_generator
  - **Mac:** appviewx_est_client_installer_generator.app
- appviewx_est_client_installer_generator.app
- README.md

Configuring EST Client

1. Navigate to the following extracted folder:
   - **For Linux and Mac:** appviewx_est_client_installer_generator > input
   - **For Windows:** AppViewX_EST_Windows_Client > Generator > input
2. Replace the following files from the input folder with your authentication key and certificate with the same names. Ensure that the key file is not encrypted and the certificate file is in .crt format. (This certificate must be trusted by the EST server. The issuer certificate must be configured in the EST server setting under **Client Authentication > Issuer Certificate**):
   - est_auth.crt
   - est_auth.key
3. Open the credentials file in the Notepad editor and add the following details in two separate lines:

```
<username>

<password>
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- The username and password are the values that are configured in the agent setting under Client Authentication in the EST Agent Server Settings.
- This step is not required when the **Authentication Mode** is set to *Only Certificate TLS* in AppViewX EST agent setting.
- When the Fallback credentials under Client Authentication is set to *Logged on user credentials* on the server side, enter the AppViewX web username and password (used to login into the AppViewX web page/UI) in the credentials file. (This feature is only available from AppViewX server version Ganga - 2022.1.0 and later)

4. Open the secure_config.json file and edit the configuration file.
   The details of the parameters are as described:

   Structure of the secure_config.json file:

   - **General parameters**: Comprises the general configuration parameters such as allowed domain names and the option for silent uninstallation.
   - **EST server parameters**: In this section, you can provide the configuration details of EST server such as hostname, port number, and agent name (which represents the agent name in the server settings) specific to the certificate type.
   - **Certificate parameters**: For the mentioned certificate_type in the EST server parameters, you can provide certificate-specific details in this section. These details include CSR parameters, SAN details, and the configuration related to re-enrollment.

   For more details regarding the parameters, see the following tables:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Figure 3. Sample secure_config.json file

```
{
  "is_sso_required": false,
  "override_secure_config_certificate_section": false,
  "silent_uninstallation": true,
  "allow_manual_enrollment": true,
  "est_servers": [
    {
      "certificate_type": "machine",
      "host_name": "192.168.73.193",
      "port": 30021,
      "agent_name": "est"
    },
    {
      "certificate_type": "user",
      "host_name": "192.168.73.193",
      "port": 30021,
      "agent_name": "est"
    },
    {
      "certificate_type": "others",
      "host_name": "192.168.73.193",
      "port": 30021,
      "agent_name": "est"
    },
    {
      "certificate_type": "auth",
      "host_name": "192.168.73.193",
      "port": 30021,
      "agent_name": "est"
    }
  ],
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the General Section parameters

Parameter	Type	Mandatory	Description
silent_uninstallation	Boolean	No	This field is accessed by secure_config.json during the installation process. • By default, this value is *false*. You will be prompted to uninstall the previous client. • If the value is *true*, then you will be prompted to uninstall the previously installed versions.
allow_manual_enrollment	Boolean	No	• By default, this value is *true* allowing you to enroll and re-enroll the certificates using the commands. • If the value is *false*, then the certificates are allowed to enroll and re-enroll the certificates using the commands.

install_for_all_users	Boolean	No (applicable only for Windows)	Accessed by secure_config.json. This field is used to avoid multiple installations of AppViewX client in multiple places.
			• By default, this value is *false*, then
			  • no admin access is required and the client is installed in HKEY_LOCAL_MACHINE registry
			  • EST task schedulers are not created as this task creation requires admin privileges. This option is mainly used for non C:\ folder installation and manual EST auto commands.
			• If the value is *true*, then you must have admin privileges to install. AppViewX client is installed in the HKEY_CURRENT_USER registry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameter	Type	Mandatory	Description
			• If the client is reinstalled, the installed path is retrieved from the Windows registry based on this flag, and the client is uninstalled before being reinstalled.
override_user	Boolean	No	The Boolean value determines the certificate parameters to be considered during installation. • By default, this value is *false*. • If the value is *true*, then you can override the config.json's certificate parameters value over the secure_config.json's value. This is applicable only for the certificate section field values. Precedence table based on this field is as given below.

Precedence table for Certificate Section based on the *override_user* Flag

override_user flag	Values in secure_config.json	Values in config.json	Result - Values taken from
FALSE	Present	Absent	secure_config.json
	Absent	Present	config.json
	Absent	Absent	Do nothing
	Present	Present	secure_config.json
TRUE	Present	Absent	secure_config.json
	Absent	Present	config.json
	Absent	Absent	Do nothing
	Present	Present	config.json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EST Server section parameters

Parameter	Type	Mandatory	Description
certificate_type	String	Yes	This parameter is **case-insensitive**. It can have the following values: • auth • user • machine • others Duplicate values are not allowed.
host_name	String	Yes	A valid IP/FQDN provided in EST endpoint configuration. For SAAS, use Cloud Connector IP/FQDN as provided in the endpoint configuration.
port_number	Integer	Yes	Can have a value between 1 and 65535. Make sure it matches the port number specified in the EST endpoint configuration on the AppViewX GUI (Default port is 30021).
path_seg	String	Yes	This is the EST endpoint setting name from the AppViewX GUI. It must not include any spaces. If the agent name is not present in either the secure_config.json or config.json, the defaultEST agent name is used.

After configuring the **server** and the **general** parameters, the **certificate** section must be configured. The following image provides the example of the certificate section. The certificate section must be configured for the certificate_types mentioned in the EST server section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
  "certificate_id": 2,
  "certificate_type": "others",
  "common_name": "others.appviewx.com",
  "reenrollment_trigger_before_no_of_days_of_expiry": 365,
  "certificate_country": "AU",
  "certificate_province": "TN",
  "certificate_locality": "City",
  "certificate_organization": "Limited",
  "certificate_organization_unit": "IT",
  "certificate_email_address": "test@appviewx.com"
},
```

Field descriptions for the Certificate Section parameters

Parameter	Type	Mandatory	Description
certificate_type • **Linux and Mac:** appviewx_est_client_installer_generator • **Windows:** Generator	String	Yes	This parameter is **case-insensitive**. It can have the following values: • *auth*: Generates the common name based on the est_auth.crt auth file present in the input subfolder within the folder mentioned: • *user*: Generates Logged in Username as CN for the CSR. • *machine*: Generates logged in machine name as CN for the CSR. • *others*: Generates configured common_name as CN for the CSR and installs the certificate in the key_store.
certificate_id	Integer	Yes	Contains the certificate ID. Duplicate values are not allowed.
certificate_country	String	No	The country code must be in ISO standards (2-letter code).
certificate_province	String	No	The province name; it can be up to 128 characters.
certificate_locality	String	No	The locality name; it can be up to 128 characters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameter	Type	Mandatory	Description
certificate_organization	String	No	The organization name; it can be up to 64 characters.
certificate_organizationUnit	String	No	The organization unit; it can be up to 64 characters.
reenrollment_trigger_before_no_of_days_of_expiry	Integer	Yes	The number of days before re-enrollment can be triggered. The value can be up to 36500.
common_name	String	Yes (only for **others** certificate type)	Cannot have more than 64 characters.
allowed_san_domains	List [string]	No	This field can only be used in secure_config.json and will not be considered even if it is provided in config.json. Must contain proper domain names. For example, if the **allowed_san_domains** contain ["a.com","b.com","c.com"] and the **san_dns_names** contains ["test.a.com","test.b.com","test.c.com", "test.d.com"], then only the first three domain names from **san_dns_names** are considered and used. If **allowed_san_domains** parameter is absent in the file, then all the SAN restrictions are removed.
san_dns_names	List [string]	No	Cannot have more than 255 characters - Must be a proper FQDN
san_ip_addresses	List [string]	No	Must be valid IP addresses.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameter	Type	Mandatory	Description
store_name *[Applicable for Windows ONLY]*	String	No	If the certificate type is *others*, then the store name must be either *user* or *machine*.
certificate_email_address	String	No	Cannot have more than 255 characters - Must be a valid email address
custom_values	Custom values provided are framed during EST client run time to frame the field values that trigger the enrollment. They can be accessed by both config.json and secure_config.json. The custom values are defined below: Example to use custom_values is "custom_values":[{"field_name":"common_name", "base_value":"$MACHINE", "additional_value": ".appviewx.com", "operation":"prepend"}] Here the common will be changed to machinename.appviewx.com		
field_name	N/A	Yes	Common_name or san_rfc822 name to which the values must be added.
base_value	N/A	Yes	Value can be $MACHINE or $USER or any other value. • If value is $MACHINE, then the machine name is considered. • If value is $USER, then it will be the machine logged in user name.
additional_value	N/A	Yes	Any specific value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameter	Type	Mandatory	Description
operation	N/A	Yes	Values can be *append* or *prepend*. • If the value is *append*, then the final value is fieldvalue = base_value + additional_value. • If the value is *prepend*, then the final value is fieldvalue = additional_value +base_value. If the field name is san_rfc822name, then the final value is added in CSR's SAN value.

Note: The above parameters are accessed by config.json and secure_config.json files unless specified.

Note:

- Having all types in the config.json file is not mandatory. You can retain only the necessary type and remove the rest. For example, if you want to enroll only User CERT, then you can delete *machine* and *other* types from the list.
- If there are any absent fields or parameters in the secure_config.json, they are disregarded and not enforced as mandatory. This is because you can set up the missing fields in the config.json file located in the installer folder.

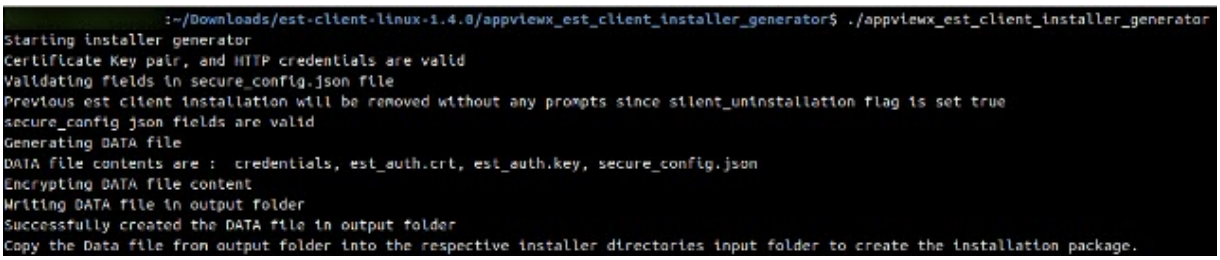
Running Generator and Installer on Linux

Running EST Installer Generator

1. Go to the appviewx_est_client_installer_generator folder.
2. Right-click and select **Open in terminal**.
3. Run:

```
./appviewx_est_client_installer_generator
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Troubleshooting: If the output has errors, correct the values or parameters in the secure_config.json file and re-run the command until it successfully creates the DATA file. The DATA file is created in the output subfolder within the appviewx_est_client_installer_generator folder.

4. To create the installation package, go to appviewx_est_client_installer_generator > output and copy the DATA file present there and paste it into the appviewx_est_client_installer > input folder.
5. In the same input folder, verify the config.json file.

Note: Repeat the steps for the secure_config.json file as mentioned in the Section Configuring EST Client . If you want to modify the values set by the admin in secure_config.json, you can do so in config.json provided the **override_user_flag** is set to *true*. (See Precedence table for Certificate Section based on the *override_user* Flag.)

The EST client folder (AppViewX_EST_Installer) can be distributed to the client machines for installing the AppViewX EST client. The admin only needs to generate the installer once, which can then be shared with other users. The DATA file within the AppViewX_EST_Installer folder contains all the configuration details from the generation of the AppViewX EST client installer.

Installing EST Client

This task must be completed on each machine where the EST client installation is required, while the generation of the installer is a one-time process carried out by the admin.

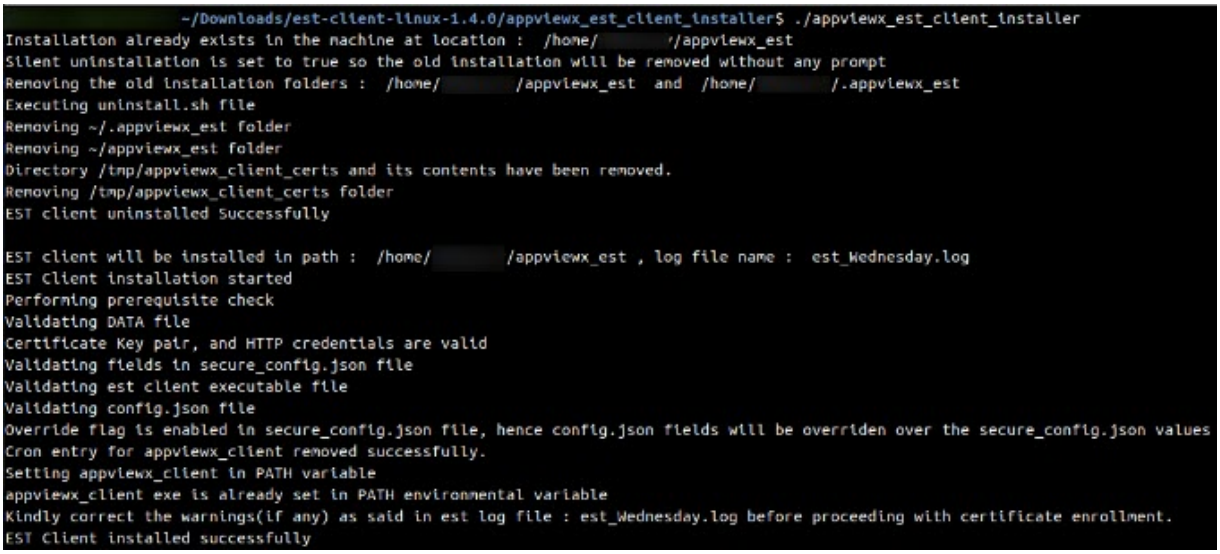
Only if the **override_user** flag is set to *true* when generating the EST agent can you modify the **certificate** section in the config.json file located within the appviewx_est_client_installer > input folder.

To install EST client:

1. Go to the appviewx_est_client_installer folder, right-click and select **Open in terminal**.
2. Run:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
./appviewx_est_client_installer
```



- If there are errors in the config.json file, then correct the errors and run the installer again. (The log files for the installation are saved in the appviewx_est_client_installer > appviewx_est_client_installer.log file.)
- During the installation process, all fields in the secure_config.json and config.json files are verified and compared according to the **override_user** flag outlined in the table below. If any mandatory fields are found to be missing or invalid, all errors are gathered and presented to you for correction before proceeding with enrollment and installation.
- If there is an existing client installation in the home folder and the **silent_uninstallation** flag is enabled, you will not receive a prompt for uninstallation. However, if the flag is disabled, you will be prompted to uninstall the previous installation.

  If you enter Y and continue, you will be asked to remove the old installation folders. If you confirm by entering Y, the old installation is deleted thus allowing the new installation to proceed; otherwise, the program will exit.

- The EST client is automatically installed in your Home folder. The following folders are created in the Home folder after installation is complete:
  - appviewx_est
  - .appviewx_est
- Certificates are stored in the keystore folder under /Home/<username>/.appviewx_est/key_store/key_store. This can only be found after fetching the required certificates from the server.
- If you accidentally deleted the appviewx_est and .appviewx_est home folders, then the installation is considered as a new installation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- You can run the appviewx_client command from any location on the machine as this executable is part of the environment PATH variable. To enable this functionality, make sure to reload the .bashrc file, which is required only during the initial installation. You can do this by running the source ~/.bashrc command or by closing and reopening the terminal.
- The most recent log file for the AppViewX EST client is named est_<CurrentDayName>.log (for example, est_Friday.log), while older files are stored based on their days. These logs are located within the appviewx_est directory in the Home folder.

3. To install with cron expression, run:

```
./appviewx_est_client_installer -cron "* * * * *"
```

- This command installs the EST client and sets up a crontab on the Linux/Mac machine using the specified cron expression. The Linux/Mac crontab daemon then automatically runs the appviewx_client est auto command at the designated time interval.
- The above cron expression is a sample command to trigger the EST auto after every minute.
- To verify the cron jobs, run:

```
crontab -l
```

The generated installation logs are captured in appviewx_est_client_installer.log located in the same folder where the installer file is located.

Verifying EST Client Installation

1. To list the commands to be run for verification, run:

```
appviewx_client -h
```

```
                    :~/Downloads$ appviewx_client -h
Log limit 100000 number of lines hasn't reached so updating in same log file
Usage:
  appviewx_client [command]

Available Commands:
  est                   est protocol based certificate enrollment and reenrollment
  help                  Help about any command
  keystore              keystore
  updateAuthCertificate Update the Authentication Certificate and key
  updateAuthCredentials Update the Authentication Credentials - username and password
  version               version

Flags:
  -h, --help   help for appviewx_client

Use "appviewx_client [command] --help" for more information about a command.
                    :~/Downloads$
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. For more information about a command, run:

```
appviewx_client --help
```

If the command does not work for any reason, then go to the ~/appviewx_est folder and run one from the following commands:

- To list the commands, run:

```
./appviewx_client -h
```

- For more information about a command, run:

```
./appviewx_client --help
```

Triggering Enrollment Request

1. Go to the Home/appviewx_est folder, right-click and select **Open in Terminal**.
2. Run:

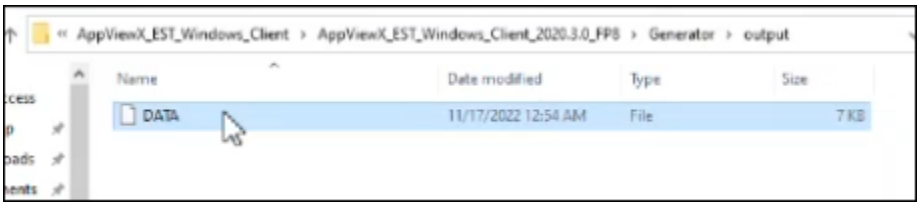
```
appviewx_client est auto
```

Running Generator and Installer on Windows

Running EST Installer Generator

1. Go to the AppViewX_EST_Windows_Client > Generator > input extracted folder.
2. Run appviewx_est_client_installer_generator.exe (right-click the file and select **Run as administrator**).
   A folder named output is generated in the same directory. If the output folder is not created, review the secure_config.json file for potential errors and repeat the step.
3. Go to the AppViewX_EST_Windows_Client > Generator > output folder.
   A file named DATA is created as a result of the execution of the above installer file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. Copy this DATA file and place it in the AppViewX_EST_Installer > input folder.
5. In the same input folder, verify the config.json file.

> **Note:** Repeat the steps for the secure_config.json file as mentioned in the Configuring the EST Client section. If you want to modify the values set by the admin in secure_config.json, you can do so in config.json provided the **override_user** flag is set to *true*. See the Precedence table for Certificate Section based on the *override_user* Flag).

6. Go to the Scheduler folder (AppViewX_EST_Installer > Scheduler) and verify the files as shown:

It contains the following details:

- triggerJobSystem.ps1: PowerShell Script for creating machine enrollment schedule task. The default trigger is at User LogOn.
- triggerJobUsers.ps1: PowerShell Script for creating user enrollment schedule task. The default trigger is at User LogOn.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attention: By default, the triggers will be in LogOn. You can customize it by following the following steps to change this to trigger at a particular time daily:

a. Open the triggerJobSystem.ps1 that is responsible for scheduling the task for *auth* and *machine* certificate. Replace the following line that triggers a task by log-on (shown in the following image) to *$trigger = New-ScheduledTaskTrigger -Daily -At HH:MM.* This triggers the task everyday at the specified time HH:MM.

b. Make the similar changes in the triggerJobUsers.ps1 file. Ensure that both tasks are scheduled with sufficient time difference between them.

```
# if ($userPolicy -eq $null) {
#     $taskDescription = read-host -Prompt "Please enter a valid user policy ("users" or "system"): "
# }

$task = Get-ScheduledTask -TaskName $taskName -ErrorAction SilentlyContinue
if ($null -ne $task) {
    Unregister-ScheduledTask -TaskName $taskName -Confirm:$false
}
if ("null" -eq $arguments) {
    $action = New-ScheduledTaskAction -Execute $executablePath
}
else {
    $action = New-ScheduledTaskAction -Execute $executablePath -Argument $arguments
}
$trigger = New-ScheduledTaskTrigger -AtLogOn
$trigger.Delay = 'PT3M'
$settings = New-ScheduledTaskSettingsSet -Compatibility Win8 -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries
$currentUser = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
# $userGroup = "users"
if ($userPolicy -eq "users") {
    $principal = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Users"  -RunLevel Highest
}

#if ($userPolicy -eq "system") {
#    $principal = New-ScheduledTaskPrincipal -UserId $YSTEM  -RunLevel Highest
#}
if ($userPolicy -eq "system") {
    $principal = New-ScheduledTaskPrincipal -GroupID "SYSTEM" -RunLevel Highest
}

$definition = New-ScheduledTask -Action $action -Principal $principal -Trigger $trigger -Settings $settings -Description $taskDescription

Register-ScheduledTask -TaskName $taskName -InputObject $definition
```

The EST client folder (AppViewX_EST_Installer) can be distributed to the client machines for installing the AppViewX EST client. The admin only needs to generate the installer once, which can then be shared with other users. The DATA file within the AppViewX_EST_Installer folder contains all the configuration details from the generation of the AppViewX EST client installer.

Installing EST Client

This task must be completed on each machine where the EST client installation is required, while the generation of the installer is a one-time process carried out by the admin.

Only if the **override_user** flag is set to *true* when generating the EST agent can you modify the **certificate** section in the config.json file located within the appviewx_est_client_installer > input folder.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

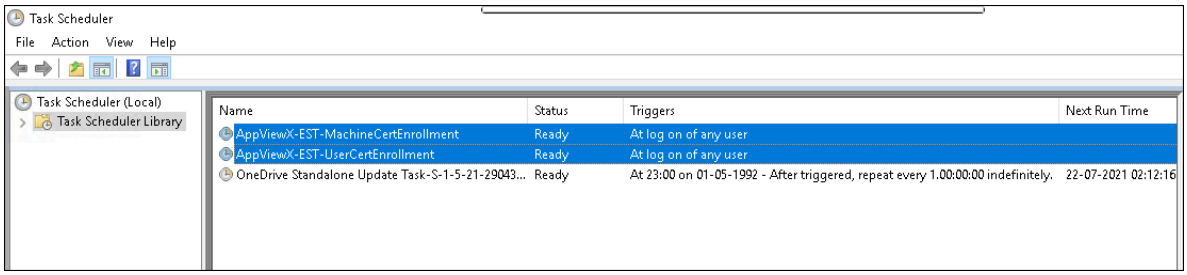
1. To install EST client:

   a. Open the AppViewX_EST_Installer folder and select the installer.bat file.

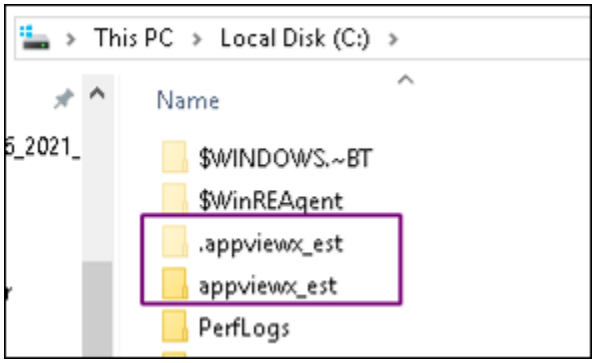
   b. Right-click and select **Run as administrator**.
   - It creates **Machine** and **User Enrollment** tasks in the Windows Task Scheduler.
   - It encrypts the software with machine-unique parameters and copies to C: drive.

2. After the installation:

   a. Create **Machine** and **User enrollment** tasks in the task scheduler.



   b. Copy the files to the C: drive

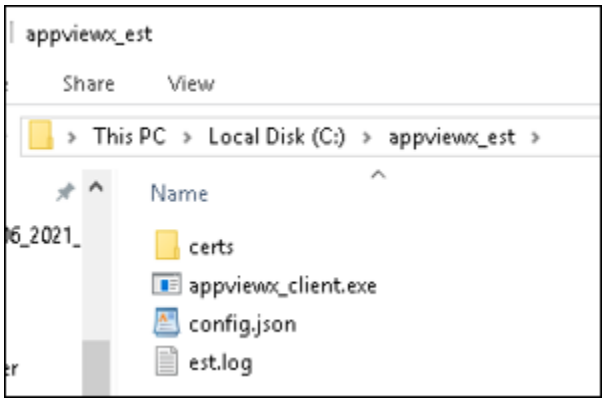


   .

> **Note:** Check if appviewx_est and .appviewx_est have all the permissions to write, read, and modify. If not, provide the necessary permissions.

   c. Validate whether the config.json file is present in C:/appviewx_est/config.json.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

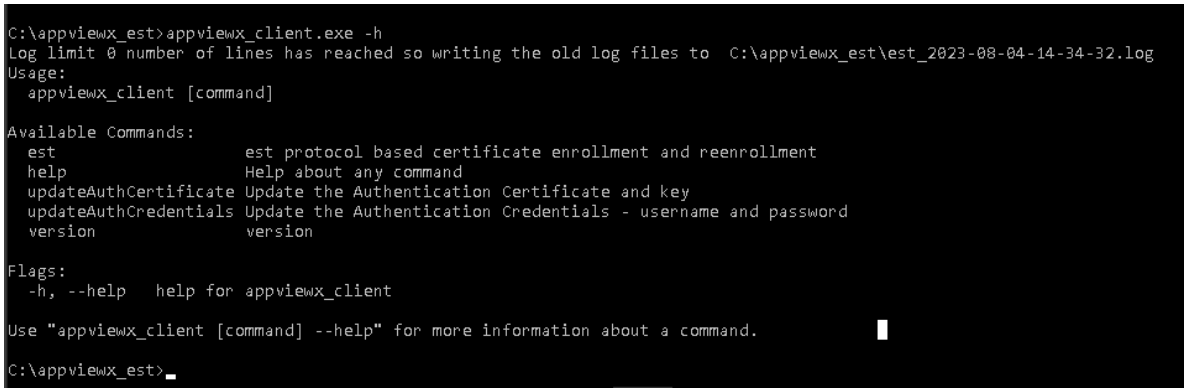


d. Open the command prompt with administrator privileges and navigate to C:/appviewx_est.

e. Run:

```
appviewx_client.exe -h
```

A list of commands is displayed to help users with different processes as shown:



3. **Note:** This agent can either be triggered automatically when you log in or can be triggered manually from the Task Scheduler.

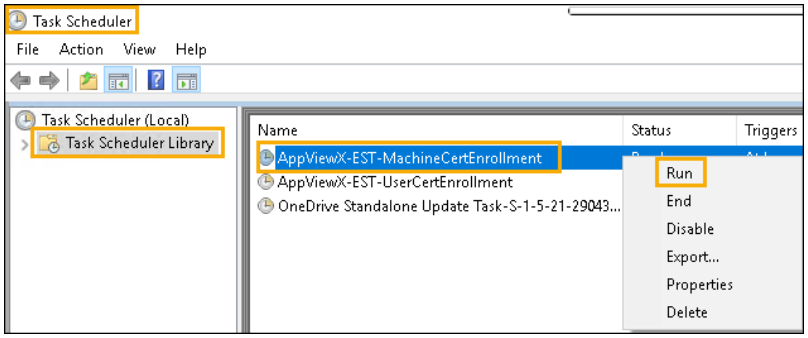
To trigger the enrollment task:

a. Open the task scheduler library, and select the AppViewX-EST-MachineCertEnrollment file. Once you log out of the system and log back in, the enrollment/re-enrollment is triggered automatically.

b. Right-click and select **Run** to run the tasks.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Only User scheduler works this way as Machine scheduler requires system user permission to run it. The certificates are installed in the store within 30 seconds.



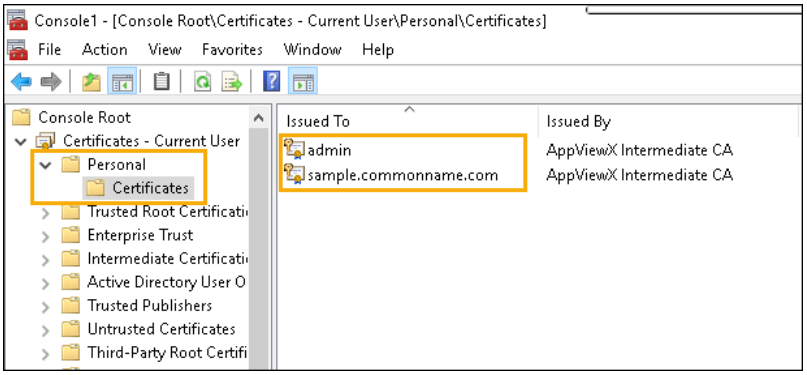
Enrollment request can be triggered by running the task from the task scheduler or can be triggered by the following steps:

1. Open the command prompt with administrator privileges, and go to C:/appviewx_est.
2. Run:

```
appviewx_client.exe est auto
```

The latest log file for the AppViewX EST client can be found in est_<CurrentDayName>.log (for example, est_Friday.log) while the old files are saved based on the day. These logs are found in the appviewx_est folder present in the C:/ drive.

The certificates are created based on the configurations provided. The **machine** type certificate can be found in the Machine certificate store whereas the **user** and the **others** type certificates are present in the User certificate store. The certificates are present in the sections as shown:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Actions using EST Client

Available Commands and their Descriptions

List of Available Commands and their Description

Available Command	Description
est	EST protocol based certificate enrollment and re-enrollment.
help	Help about any command.
keystore	Listing the certificates in the keystore.
updateAuthCertificate	Update the Authentication certificate and key. Example: `appviewx_client updateAuthCertificate --authCert “<certificate path>” --authKey “<keypath>”`
updateAuthCredentials	Update the Authentication Credentials - username and password. You are prompted to enter the username and the password.
version	Version details.

Auto-Enrollment and Re-Enrollment

- To perform auto-enrollment or re-enrollment, run:

```
appviewx_client est auto
```

  This enrolls certificates based on the secure_config and the config files.
- If certificates are already enrolled, then the validity of the certificates are checked against the **reenrollment_trigger_before_no_of_days_of_expiry** value present in the configuration files. If the certificate's expiry in number of days from today is less than **reenrollment_trigger_before_no_of_days_of_expiry** value, then re-enrollment will be triggered. Example: If the **reenrollment_trigger_before_no_of_days_of_expiry** value is 30 and if the certificate is going to expire in the next 20 days, then the re-enrollment will be triggered.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Manual Enrollment and Re-Enrollment

Note:

- Manual enrollment and re-enrollment are possible only if **allow_manual_enrollment** is set to *true* in the secure_config.json file.
- Before running the manual enrollment and re-enrollment commands, Linux and Mac users must navigate to appviewx_est in their home directory, while Windows users must navigate to appviewx_est in the C: drive.

- Manual enrollment and re-enrollment do not come under any certificate type mentioned in the configuration files.
- Manual enrollment is accessed through the following command:

Example 1:

```
appviewx_client est manual-enrollment csr-mode --csr-file <csr-file-complete-path> --est-server-url <est-server-url>
```

Example 2:

```
appviewx_client est manual-enrollment csr-mode --csr-file <csr-file-complete-path> --est-server-hostname <est-server-hostname> --est-server-pathseg
<est-server-pathsegment/agent name>
```

The description for every parameter is given in the following table:

Flags	Input Type	Description
--csr-file	string	Input CSR filename. For example: /home/user/test.csr
--est-server-hostname	string	EST server hostname
--est-server-pathseg	string	EST server name present in the EST server setting (default value: defaultEST)
--est-server-port	int	EST server port number configured in the EST server settings (default value: 30021)
--est-server-url	string	EST server URL present in the EST server setting page. (Not required if the hostname, port, and agent name are given.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Manual re-enrollment is triggered using two modes:
  - **csr-mode**

    Ensure that the certificate corresponding to the CSR sent is present in the inventory before triggering re-enrollment.

    Example 1:

    ```
    appviewx_client est manual-reenrollment csr-mode --csr-file <csr-file-complete-path> --est-server-url <est-server-url>
    ```

    Example 2:

    ```
    appviewx_client est manual-reenrollment csr-mode --csr-file <csr-file-complete-path> --est-server-hostname <est-server-hostname> --est-server-pathseg <est-server-pathsegment/agent name>
    ```

    Note: See the table in the manual-enrollment, for the description of these parameters.

  - **cert-mode**

    Similar to the manual re-enrollment using csr-mode, the certificates must be enrolled and must be present in the inventory before triggering re-enrollment.

    Example:

    ```
    appviewx_client est manual-reenrollment cert-mode --cert-file <cert-file-complete-path> --cert-file-type <cert-file/extension-type> --est-server-hostname <est-server-hostname> --est-server-pathseg <est-server-pathsegment/agent name> --output-privatekey-file <path-to-store-private-key> --key-size <Key-length>
    ```

    Descriptions for the flags/parameters for the manual cert-mode are as follows:

    Flags and their description

Flags	Input Type	Description
--cert-file	string	Input Certificate filename. For example: /home/user/test.crt
--cert-file-type	string	Input Certificate file types (cer, crt, pem, p7b)
--key-size	int	Key size of the generated private key. If not given, the key size is taken from the old certificate.
--output-privatekey-file	string	Output private key filename.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Flags	Input Type	Description
		Example: /home/user/output/hostname.key
--est-server-hostname	string	EST server hostname
--est-server-pathseg	string	EST server name present in the server setting (default value: defaultEST)
--est-server-port	int	EST server port number configured in the EST server settings(default value: 30021)
--est-server-url	string	EST server URL present in the EST server setting page. (Not required if hostname, port, and agent name are given)

Keystore

On Linux

- To view the list of certificates created, run:

```
appviewx_client keystore list
```

```
dhivya.v@avxpll771:~/Downloads/20230306-2022.1.0_5-Validations/toDevopsForRelease/AppViewX_EST_Linux_Client_20230306-2022.1.0_5/appviewx_est_client_installer$ appviewx_client keystore list
+-----------------------------------------------------------------------------------------------------------------------------------------------------------------+
|ID   |Common Name             |SerialNumber                                |Download Type  |Created Date                |Expiry Date                 |
+-----------------------------------------------------------------------------------------------------------------------------------------------------------------+
|0    |avxpll771.appviewx.com  |4E0F5A037572E2449160D9B9AD6E8F91             |p12            |Mon Mar 20 15:17:46 2023    |Tue Mar 19 23:59:59 2024    |
|1    |secure.appviewx.com     |1EF5F92BC76CFEDAC96EC24E7A8DF6C             |p12            |Mon Mar 20 15:17:59 2023    |Tue Mar 19 23:59:59 2024    |
+-----------------------------------------------------------------------------------------------------------------------------------------------------------------+
```

- To download the certificates based on **id** specified when using the `list` command above, run:

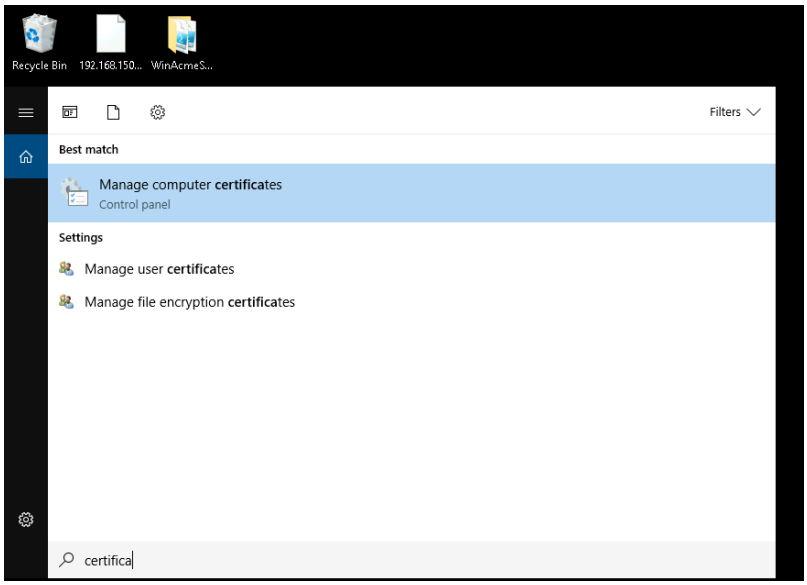
```
appviewx_client keystore download --id <id> --filepath <path to store the cert with file name and extension>
```

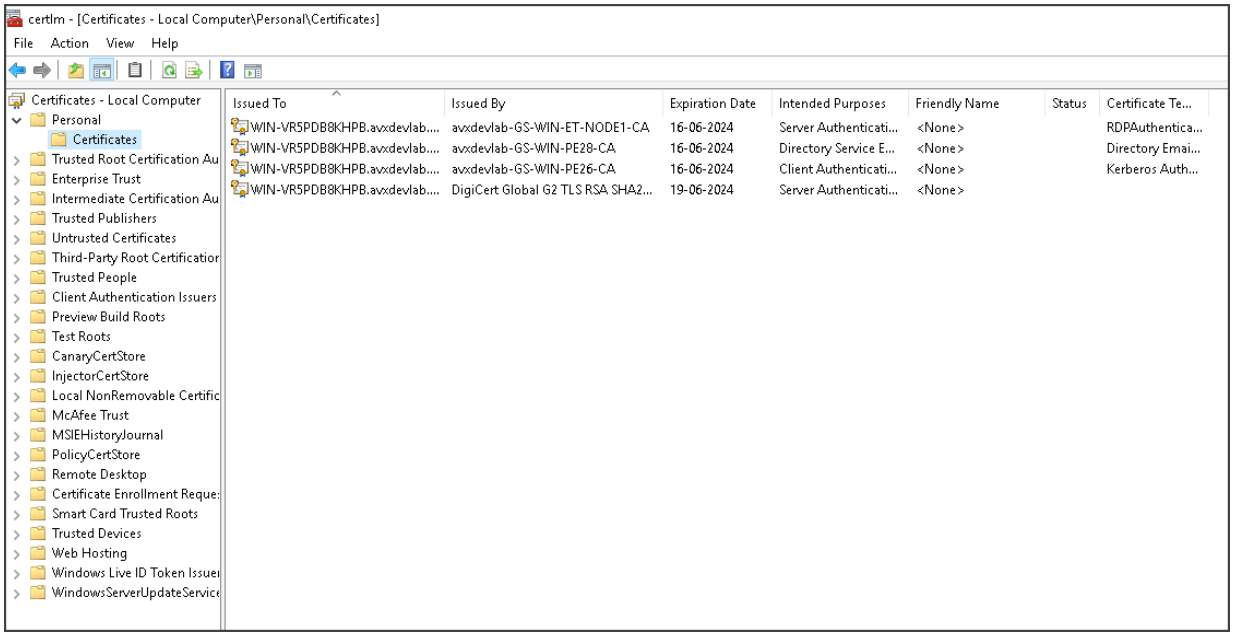
Note: To download PFX file, provide the password with --password field

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

On Windows

- To access Machine Certificate Type, go to **Start > Manage Computer Certificates**.
- To access User and Others Certificate Type, go to **Start > Manage User Certificates**.
- To view the certificates, go to **Personal > Certificates**.





Uninstalling the EST Client

The uninstall.sh is present along with the other files you downloaded and extracted as mentioned in instructions for installing the EST client. Run the uninstall.sh script in the command prompt as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
ller$ ./uninstall.sh
Removing ~/.appviewx_est folder
Removing ~/appviewx_est folder
Removing /tmp/appviewx_client_certs folder
EST client uninstalled Successfully
```

The AppViewX EST client is successfully uninstalled.

Best Practices

- **Log Reference for Troubleshooting:** For any issues related to installation, enrollment, or re-enrollment, consult the **installer logs** or **EST client logs** for detailed diagnostic information.
- **Installer Behavior and Cleanup:** The installer places the AppViewX EST Client in the user's **home directory**. It is recommended to delete the installer from the machine after successful installation to maintain security hygiene.
- **Machine Binding and Security Restrictions:** The EST client is bound to the machine on which it is installed. Transferring or using EST client artifacts (e.g., .exe files) on other machines is not permitted due to strict security controls.
- **Windows-Specific Installation Steps:**
  - Always use **installer.bat** for Windows installations to ensure proper creation of Task Scheduler entries.
  - After installation, users must sign out and then sign back in. Upon re-login:
    - **User** and **Others** certificate type enrollment will begin immediately.
    - **Machine** and **Authentication** certificate type enrollment will occur after approximately 3 minutes.
  - This timing and behavior can be customized by:
    - Modifying the Task Scheduler settings post-installation, or
    - Editing the PowerShell (.ps) file before installation.
- **Certificate Store Behavior:** Reinstalling the EST client does not delete the existing certificates from the Windows certificate store or macOS keychain.
- **CSR Parameter Configuration:**
  - To define mandatory CSR fields, update the **secure_config.json** file located in the Installer Generator folder.
  - Use the provided sample **config.json** and **secure_config.json** files as templates. Remove any unused fields based on your requirements.
- **Configuration Best Practices:**
  - Always use the Fully Qualified Domain Name (FQDN) instead of the server IP address in both **config.json**and**secure_config.json**.
  - This ensures proper communication with the EST server during enrollment and re-enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Regenerating Data After Config Updates:**
  - Any change made to the **secure_config.json** file requires the DATA file to be regenerated.
  - The installation process must be re-executed following this update.

Troubleshooting

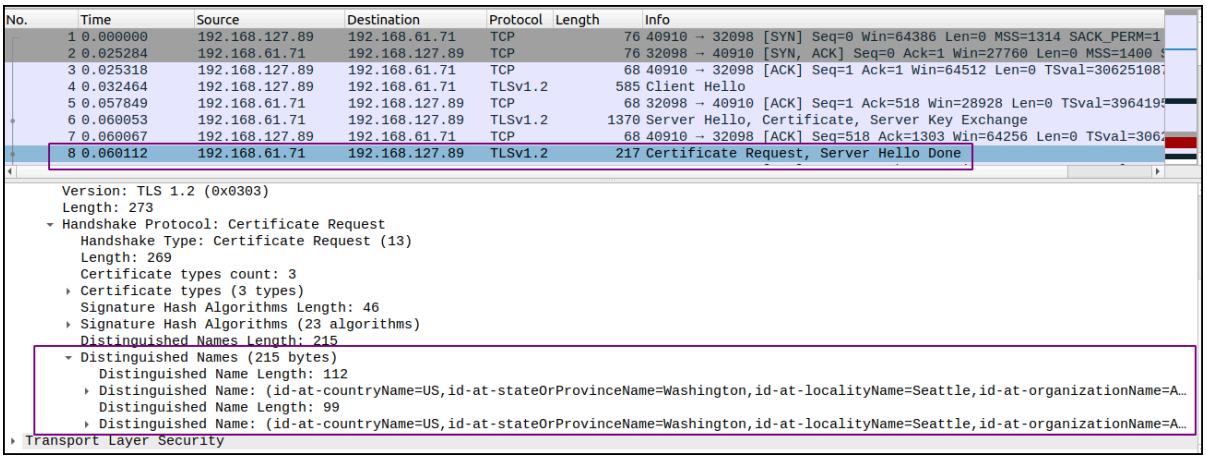
This section covers error scenarios and the troubleshooting steps only for Linux and Windows users.

Connection Errors

1. Check whether the IP address and the port number are correctly configured in the secure_config.json file located in the AppViewX_EST_Windows_Client > Generator > Input folder.
2. Verify if the firewall policies permit the connection between the EST client and the server.

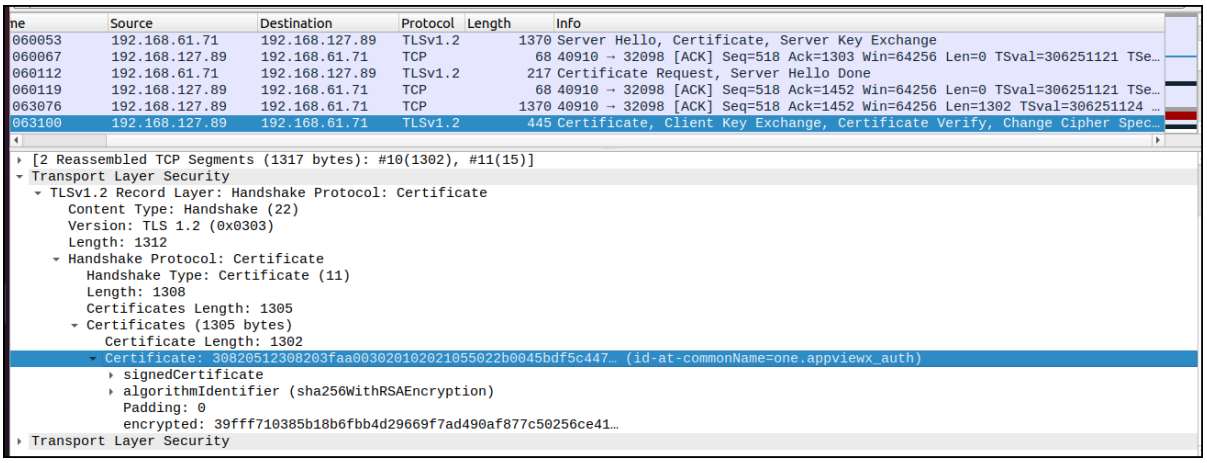
Error Code: 401 Unauthorized

1. Ensure the client sends the authentication certificate (try enrollment request from `curl` using the same client certificates).
2. Check the trusted CA added in the EST agent settings to validate whether the client authentication certificate is signed by the same CA.
3. If the client authentication certificate is signed by a CA other than AppViewX, make sure it is added in the trusted CA list from the CLI.
4. Do a TCP dump and analyze the TLS transactions between server and client to make sure the client receives the Distinguished Name of the Trusted CA.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. In the TCP dump, make sure the client sends the Authentication Certificate in the Certificate Response field.



500-Internal Server Error

1. Make sure EST service is running on the AppViewX server.
2. Check the EST server status. (Refer section: Verify EST Server Status (Enabled/Disabled).)
3. Check the EST enrollment using `curl`. (Refer section: Testing EST Enrollment by using **CURL**.)

Error Codes

Error Codes and their Descriptions

S. No.	Status Code	Error Codes	Error Messages	Description
1	500 - Internal Server Error	CERT-ENROLLMENT-001	Agent settings are not found (or) invalid for this agent	When there is no agent found for EST with the specified name.
2	500 - Internal Server Error	CERT-ENROLLMENT-002	Agent settings are not valid	When EST agent settings are invalid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
3	401 - Unauthorized	CERT-ENROLLMENT-003	Authentication failed for the auto-enrollment protocol	TLS / Basic / Digest authentication failed for the provided authentication parameters.
4	401 - Unauthorized	CERT-ENROLLMENT-006	Provided NONCE is invalid	• When TLS and HTTP auth are selected but the input does not contain any Basic auth value. • When TLS and HTTP auth is selected but the input does not contain any Digest auth value. Here Nonce is sent in the WWW-Authenticate header as per RFC.
5	500 - Internal Server Error	CERT-ENROLLMENT-007	Failure while creating nonce	When creating Nonce to send to the client in case of Digest HTTP authentication.
6	500 - Internal Server Error	CERT-ENROLLMENT-008	Certificate conversion failed	While converting the certificate contents to PKCS7 format which is to be sent as a response to the client.
7	500 - Internal Server Error	CERT-ENROLLMENT-009	Error while converting to JSON	Error during map to JSON conversion.
8	401 - Unauthorized	CERT-ENROLLMENT-010	No client certificate was obtained to perform authentication.	When a client certificate is not found in the request to perform the TLS authentication.
9	500 - Internal Server Error	CERT-EST-001	Unable to get certificates requested by the client device	Could not obtain the certificates which were requested from the agent.
10	500 - Internal Server Error	CERT-EST-003	Certificate cannot be obtained after polling from the agent.	A certificate cannot be obtained even after retrying for the provided amount of time interval.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
11	500 - Internal Server Error		CSR parameters already available for selected CA.	When there is a request already present in the certificate inventory and a similar CSR is obtained for enrollment/re-enrollment.
12	500 - Internal Server Error	CERT-ENROLLMENT-PROTOCOL-1020	Certificate enrollment failed for the provided CSR.	• Check for the request-id of the submitted CSR for further details. • Certificate or certificate creation requests may not be found to retrieve the certificate. • Exception while fetching work order mapping for the transaction ID.
13	404 - Not Found	CERT-ENROLLMENT-PROTOCOL-1019	Certificate enrollment request does not exist. Check the request sent from the AppViewX agent	The request from the EST agent is not found when received in subsystem certificate NB.
14	401 - Unauthorized	CERT-ENROLLMENT-PROTOCOL-1014	Authentication failed for the autoenrollment protocol.	When TLS authentication fails.
15	500 - Internal Server Error	CERT-ENROLLMENT-PROTOCOL-1005	Error while fetching policy settings for an agent	When obtaining group or policy details.
16	400 - Bad Request	CERT-SCEP-1011	Unable to extract CSR in the SCEP request	Occurs when the CSR extraction fails.
17	404 - Not Found	CERT-SCEP-1012	Policy is not associated with the given certificate group	When the certificate policy for the provided agent is not present.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
18	404 - Not Found	CERT-SCEP-1013	Group policy does not have the given certificate authority	All the errors from 18 to 29 are to validate the CSR parameters against policy.
19	404 - Not Found	CERT-SCEP-1014	Group policy does not have the given hash function	-
20	404 - Not Found	CERT-SCEP-1015	Group policy does not have the given key type	-
21	404 - Not Found	CERT-SCEP-1016	Group policy does not have the given key length	
22	400 - Bad Request	CERT-SCEP-1017	Given common name must end with as per the common name defined in group policy	-
23	400 - Bad Request	CERT-SCEP-1018	Given common name can not be same as the common name defined in group policy	-
24	400 - Bad Request	CERT-SCEP-1019	Given organization must match with organization defined in group policy	-
25	400 - Bad Request	CERT-SCEP-1020	Given organization unit must match with organization unit defined in group policy	-
26	400 - Bad Request	CERT-SCEP-1021	Given locality must match with locality defined in group policy	-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Codes and their Descriptions (continued)

S. No.	Status Code	Error Codes	Error Messages	Description
27	400 - Bad Request	CERT-SCEP-1022	Given state must match with the state defined in group policy	-
28	400 - Bad Request	CERT-SCEP-1023	Given country must match with country defined in group policy	-
29	404 - Not Found	CERT-SCEP-1024	Group policy does not have the given certificate type	-
30	400 - Bad Request	CERT-CSR-0002	Failed to parse CSR, validate the content.	CSR content is not proper while uploading it for submission
31	404 - Not Found	CERT-CA-0001	CA settings are not available.	CA setting selected in EST settings is not found.
32	404 - Not Found	CERT-KEY-0003	Certificate/private key retrieval failed.	DAO exception while fetching certificate.
33	417 - Expectation Failed	CERT-CSR-0005	Csr submission failed. ${ERROR_MSG}	Custom error message from CA.
34	500 - Internal Server Error		More than one data returned from collection while fetching SAN list from the DB for the given server name.	More than one entry of SAN is present for the same server name.
35	500 - Internal Server Error		Error while processing.	Hookname is not mapped with the EST agent setting. Run the DB query to add the hookname.

EST Client v1.5.4

The AppViewX EST Client automates the enrollment and renewal of SSL certificates for Linux, Windows, and macOS systems. After installation, the client automatically enrolls and renews certificates before

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

expiration according to a custom configuration. Certificates can be installed for a machine, a user, or for a certificate with a user-defined Common Name (CN).

AppViewX EST Client Installation and Usage

Once installed on any Linux or Windows machine, the EST Client allows users to enroll certificates based on the required type—machine, user, or other.

EST Client 1.5.4 Features

Using PowerShell Scripts in the AppViewX EST Client

- Custom PowerShell scripts can be added to the AppViewX_Installer/Resources folder before installing the EST Client. After installation, all files from this package are copied to the C:\appviewx_est folder.
- After certificate enrollment, the specified PowerShell scripts are automatically executed to bind the enrolled certificate to the service defined within each script.
- The `certificate_type` can be **machine**, **user**, or **others**. Based on the `certificate_type`, the corresponding enrolled certificate is used to bind to the appropriate Remote Desktop (RD) service.
- Multiple scripts can be configured to run for a single certificate type.
- To enable post-enrollment script execution, add a **post_certificate_creation** section to the **config.json** file located in C:\appviewx_est. This ensures the designated PowerShell scripts run immediately after certificate creation.

```
"post_certificate_creation": [
{
"certificate_type": "machine",
"script_path": "C:\\appviewx_est\\RDSCertBindWithRestart.ps1",
"script_type": "powershell"
},
{
"certificate_type": "machine",
"script_path": "C:\\appviewx_est\\UploadCAChain.ps1",
"script_type": "powershell"
}
]
```

- The following powershell scripts have been validated from AppViewX:
  - Certificate binding to RD Services
  - Uploading enrolled certificate’ intermediate and root to the client machine's trust store.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enhanced Security

All EST Client executables, Scheduler creation PowerShell scripts, and DLLs are now code-signed.

Improved Windows EST Client Functionality

- **Automated Machine Scheduler:** The Machine scheduler in the EST Windows Client now triggers automatically one minute after installation and subsequently every 12 hours, without requiring a machine logout or login. Refer the script triggerJobSystem.ps1.
- **Windows 11 24H2 Compatibility:** Issues related to deprecated WMIC commands in Windows 11 24H2 have been resolved by removing all instances where these commands were used.
- **Certificate Re-enrollment Logic:** If an enrolled certificate is removed from the Windows Keystore, the EST Client will now enroll the certificate during its next execution.

Validated Windows Versions

The EST Windows Client has been validated on the following Windows versions:

- Windows 10
- Windows 11 23H2
- Windows 11 24H2
- Windows Server 2019 and 2022

Note: The EST Windows Client is now supported on Azure VMs. However, it is not supported on Windows 7 and Windows 8 machines, as these have reached their End of Life (EOL).

Powershell Scripts validated in EST Client 1.5.4:

triggerJobSystem.ps1

Note: The machine scheduler which is triggered automatically once EST Client installation is complete and is triggered regularly every 12 hours.

```
param(
   [Parameter(Mandatory = $false, Position = 1)][string]$taskName = "AppViewX-EST-MachineCertEnrollment",
   [Parameter(Mandatory = $false, Position = 2)][string]$taskDescription = "This task Installs Certificates issued via AppViewX in
Machine Store",
   [Parameter(Mandatory = $false, Position = 3)][string]$userPolicy = "system",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    [Parameter(Mandatory = $false, Position = 4)][string]$executablePath = "powershell",
    [Parameter(Mandatory = $false, Position = 5)][string]$arguments = "-ExecutionPolicy Bypass -WindowStyle Hidden
 C:\appviewx_est\appviewx_client.exe est auto"
)
# .Net methods for hiding/showing the console in the background
Add-Type -Name Window -Namespace Console -MemberDefinition '
[DllImport("Kernel32.dll")]
public static extern IntPtr GetConsoleWindow();

[DllImport("user32.dll")]
public static extern bool ShowWindow(IntPtr hWnd, Int32 nCmdShow);
'
function Hide-Console
{
    $consolePtr = [Console.Window]::GetConsoleWindow()
    #0 hide
    [Console.Window]::ShowWindow($consolePtr, 0)
}
#Hide-Console
# if ($taskName -eq $null) {
#     $taskName = read-host -Prompt "Please enter a proper task name: "
# }
# if ($taskDescription -eq $null) {
#     $taskDescription = read-host -Prompt "Please enter a valid task description: "
# }
# if ($executablePath -eq $null) {
# $executablePath = read-host -Prompt "Please enter a valid executable path: "
# }
# if ($userPolicy -eq $null) {
#     $taskDescription = read-host -Prompt "Please enter a valid user policy ("users" or "system"): "
# }

$task = Get-ScheduledTask -TaskName $taskName -ErrorAction SilentlyContinue
if ($null -ne $task) {
    Unregister-ScheduledTask -TaskName $taskName -Confirm:$false
}
if ("null" -eq $arguments) {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    $action = New-ScheduledTaskAction -Execute $executablePath
}
else {
    $action = New-ScheduledTaskAction -Execute $executablePath -Argument $arguments
}

$startTime = (Get-Date).AddMinutes(1)

# Trigger: every 1 minute, for 1 day
$trigger = New-ScheduledTaskTrigger -Once -At $startTime `
    -RepetitionInterval (New-TimeSpan -Hours 12) `
    -RepetitionDuration (New-TimeSpan -Days (365*60))

$settings = New-ScheduledTaskSettingsSet -Compatibility Win8 -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries
$currentUser = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
# $userGroup = "users"
if ($userPolicy -eq "users") {
    $principal = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Users"  -RunLevel Highest
}

#if ($userPolicy -eq "system") {
#    $principal = New-ScheduledTaskPrincipal -UserId SYSTEM  -RunLevel Highest
#}
if ($userPolicy -eq "system") {
    $principal = New-ScheduledTaskPrincipal -GroupId "SYSTEM" -RunLevel Highest
}

$definition = New-ScheduledTask -Action $action -Principal $principal -Trigger $trigger -Settings $settings
 -Description $taskDescription

Register-ScheduledTask -TaskName $taskName -InputObject $definition

$task = Get-ScheduledTask -TaskName $taskName -ErrorAction SilentlyContinue

if ($null -ne $task) {
    Write-Output "Created scheduled task: '$($task.ToString())'."
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
else {
    Write-Output "Created scheduled task: FAILED."
}
```

RDSCertBindWithRestart.ps1

Note: RDP connections are terminated when the certificate binding is updated. The updated certificate will be visible to the user before they connect to the machine via RDP. To avoid chain issues when reconnecting, users must have the Trust chain certificates of the enrolled certificate on their machine.

```
param (
    [string]$newCertThumbprint
)
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Thumbprint -eq "$newCertThumbprint" }
Add-Type -AssemblyName System.Security
$key = [System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($cert)
$un= $key.Key.UniqueName
$keyPath     = "C:\ProgramData\Microsoft\Crypto\Keys\$un"
$acl = Get-Acl $keyPath
$rule = New-Object System.Security.AccessControl.FileSystemAccessRule("NETWORK SERVICE","FullControl","Allow")
$acl.AddAccessRule($rule)
Set-Acl -Path $keyPath -AclObject $acl
$hex = $cert.Thumbprint -replace ' ', ''
$bin = for ($i=0; $i -lt $hex.Length; $i+=2) { [Convert]::ToByte($hex.Substring($i,2),16) }
# Write binary value into registry
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp"
 -Name "SSLCertificateSHA1Hash" -Value $bin -Type Binary
Restart-Service TermService -Force
```

ChainCertificatesImport.ps1

Note: Download the intermediate and root certificates from the AppViewX inventory. Rename them to Issuing-CA.crt and Root-CA.crt, respectively. This will ensure they are automatically uploaded to the intermediate certificate store.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
$CertDirectory = "C:\appviewx_est"
$RootCertFile = "Root-CA.crt"
$IntermediateCertFile = "Issuing-CA.crt"

# Build full paths
$RootCertPath = Join-Path -Path $CertDirectory -ChildPath $RootCertFile
$IntermediateCertPath = Join-Path -Path $CertDirectory -ChildPath $IntermediateCertFile

# Validate files exist
if (!(Test-Path $RootCertPath)) {
    Write-Error "Root certificate file not found: $RootCertPath"
    exit 1
}
if (!(Test-Path $IntermediateCertPath)) {
    Write-Error "Intermediate certificate file not found: $IntermediateCertPath"
    exit 1
}

# Import Root Certificate
Write-Output "Importing Root certificate: $RootCertPath"
Import-Certificate -FilePath $RootCertPath -CertStoreLocation Cert:\LocalMachine\Root | Out-Null

# Import Intermediate Certificate
Write-Output "Importing Intermediate certificate: $IntermediateCertPath"
Import-Certificate -FilePath $IntermediateCertPath -CertStoreLocation Cert:\LocalMachine\CA | Out-Null

Write-Output "Certificates imported successfully."
```

EST Micro CA (Standalone Server)

- Configuring EST Micro CA (Standalone Server)
- Configuring Azure IoT Hub in AppViewX

Overview

Micro CA is a standalone, lightweight Certificate Authority (CA) solution purpose-built for environments where traditional enterprise-grade CAs may be too heavy, complex, or resource-intensive. It is particularly

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

suited for IoT devices, edge computing deployments, and distributed systems that require secure communication and identity verification but operate under resource or connectivity constraints.

Key Features

- **EST Protocol:** Operates entirely on the Enrollment over Secure Transport (EST) protocol for seamless certificate issuance and renewal.
- **Intermediate CA:** Functions as an intermediate CA, deriving its trust from a central Root CA via the AppViewX PKI-as-a-Service (PKIaaS) platform.
- **Offline Capability:** Ability to issue certificates entirely offline.
- **Visibility & Traceability:** Provides comprehensive visibility and traceability of all issued certificates, ensuring compliance and audit readiness.

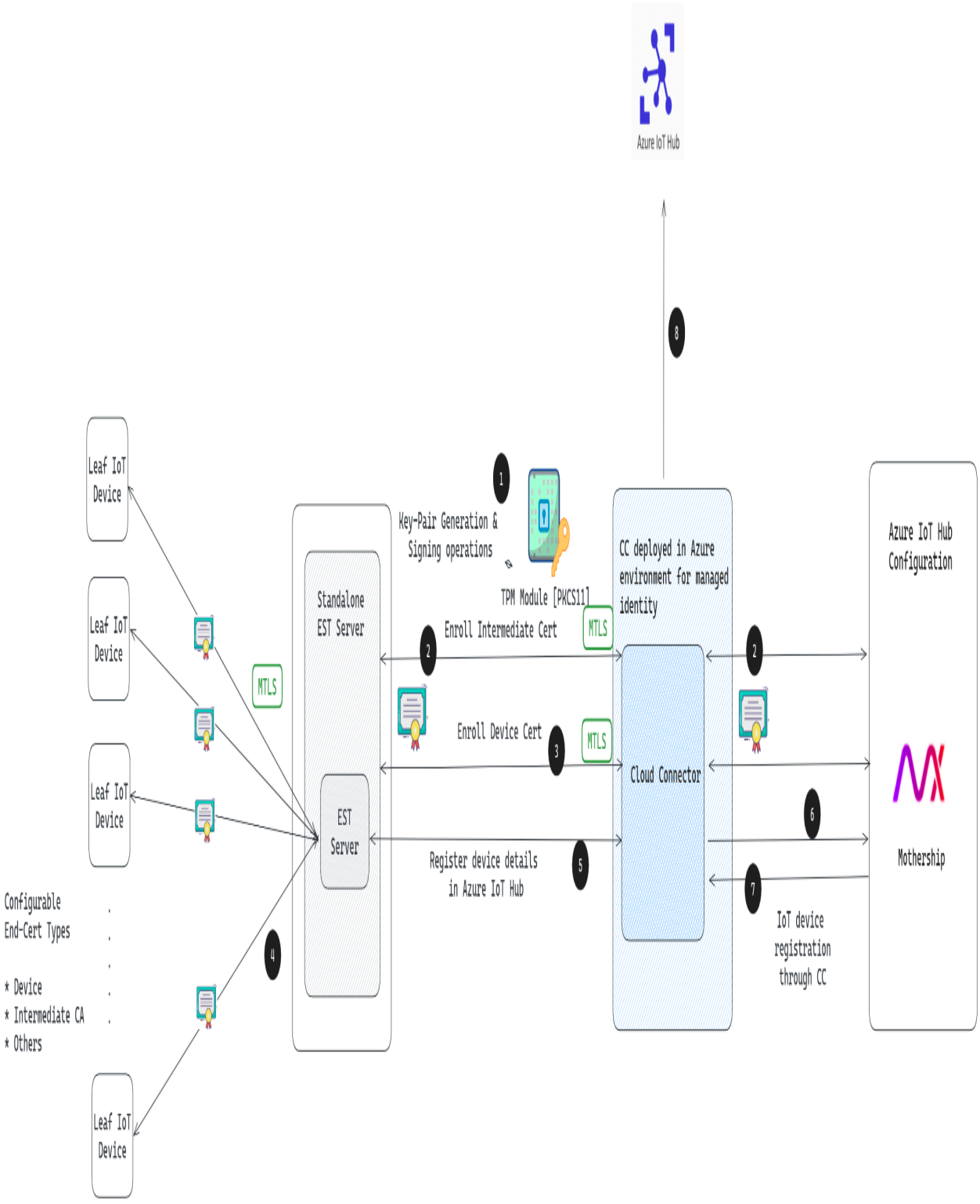
Need for Micro CA

Micro CA is designed for optimal performance in environments with limited resources, offering robust and secure certificate management.

- **Optimized for Constrained Environments:** Operates reliably on systems with 2GB RAM and 32GB storage, with a software footprint under 200MB.
- **Secure Key Management:** Utilizes PKCS#11 for secure key generation and signing through TPM (Trusted Platform Module) or HSM.
- **Offline & Remote Ready:** Supports manual intermediate CA and full certificate issuance, even in offline mode.
- **Azure IoT Integration:** Automatically updates certificate thumbprints and metadata in Azure IoT Hub.
- **Lightweight EST Client:** Features a custom Go-based client that provides full EST functionality with minimal resource consumption.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Micro CA Architecture



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Architecture key points explained

Key Points	Description
1	The EST Standalone server generates a key pair using the TPM module and initiates a certificate enrollment request to the AppViewX EST Server via the EST protocol, utilizing mTLS authentication. The Certificate Signing Request (CSR) is generated based on configurable parameters from the configuration file.
2	AppViewX processes this request and issues an Intermediate CA certificate, leveraging a Sub-CA template configured in the PKIaaS Native CA. Upon reception, the EST Standalone server uses this Intermediate CA certificate to sign CSRs and locally issue certificates for devices or subordinate CAs.
3	Similarly, device certificate CSRs are generated and issued via AppViewX PKIaaS with a template for unlimited validity (31/12/9999) and stored on the device for various device-related use cases.
4	The EST Standalone Server supports three configurable endpoints, each of which can be exposed on a customizable port. Key certificate attributes such as `Extended Key Usage`, `Key Usage`, `Path Length Constraint`, `isCA` flag, and `Azure IoT Hub` settings are defined through two configuration files. When an IoT device initiates a certificate request to the EST Standalone Server (Micro CA), it is authenticated via mTLS. The EST Standalone Server then signs the CSR using its Intermediate CA and issues the device certificate.
5—8	After issuance, the certificate thumbprint and relevant metadata are calculated and forwarded to the Cloud Connector (CC). The CC, using Managed Identity authentication, updates the Azure IoT Hub. The Micro CA also offers the option to directly update Azure IoT without routing through AppViewX.

Configuring EST Micro CA (Standalone Server)

Prerequisites for EST server

- **AppViewX**
  - AppViewX PKIaaS CA configured in AppViewX, with the capability to issue a Sub-CA certificate.
  - Service account configured.
- **Linux end machine with Sudo access.**
  - Connection to AppViewX CC to issue the intermediate certificate and update the Azure IoT Hub.
- Azure credentials and access to the Azure portal from the end machine, if Azure IoT hub needs to be updated directly from the end machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EST Server Setup and Execution

1. **Configure the API and Server Settings:** Modify the APIconfig and config.json files according to the required configuration. Example settings are provided below.
2. **Start the Server:**

   a. Run the EST server using the following command:

   ```
   sudo ./ESTSERVER
   ```

   b. Print and debug the log files which are stored in the same folder

   To print logs in the terminal:

   ```
   --logToTerminal
   ```

   To add debug logs:

   ```
   --debugMode
   ```

3. **Access the Exposed APIs:**
   - The API endpoints are available based on the `end_certificate` configurations in the **config.json** file.
   - For example, if the `end_point_name` is configured as ***device***, the EST URL will be:

     *https://<hostname>:<port-number>/.well-known/est/**device**/simpleenroll*

   - Each endpoint name exposes a different URL, which lets the user obtain certificates based on its specific configuration.

Once configured, the server listens and issues certificates using the intermediate certificate. The issued certificates are stored in the folder named IssuedCerts within the same server directory.

APIconfig File Configuration

Sample Configuration:

```
{
  "appviewx_hostname": "<AppViewX/CC Hostname>",
  "appviewx_port_number": <HTTPS Port Number - Appviewx/CC>,
  "ca_setting_name": "<AppViewX PKIaaS CA settings name>",
  "template_name": "<AppViewX PKIaaS sub ca template name>",
  "issuer_name": "<AppViewX PKIaaS issuer name>",
  "ca_name": "AppViewX PKIaaS Native",
  "intermediate_cert_validity_in_days": <Intermediate certificate validity>,
  "appviewx_group_name": "<Appviewx group to issue the certificate>",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "service_account_client_id": "<Appviewx service account id>",
  "service_account_client_secret": "<Appviewx service account secret>",
  "azure_hub_url": "<Azure IoT hub url>",
  "azure_hub_key": "<Azure IoT hub key>",
  "azure_hub_policy_name": "<Azure IoT hub Policy Name>",
  "azure_token_validity": <Token validity in seconds>,
  "poll_count": <Poll Count>,
  "poll_interval":  <Poll Interval in seconds>,
  "update_azure_iot_hub_from_standalone_server":  <true/false>
}
```

Field Description for the APIconfig File

Field	Description
appviewx_hostname	Hostname or IP address of the AppViewX API endpoint (If using a CC then use the CC's hostname).
appviewx_port_number	Port number where the AppViewX service is running (If using a CC then use the CC's port number—30020).
ca_setting_name	Name of the CA settings configured under CA Configurations in CERT+.
template_name	Name of the AppViewX PKIaaS Sub-CA template to issue intermediate CA certificates.
issuer_name	Name of the AppViewX PKIaaS issuer.
appviewx_group_name	Certificate Group in AppViewX that is used for issuing intermediate CA certificates.
service_account_client_id	Client ID for authentication to AppViewX using a service account.
service_account_client_secret	Client secret for authenticating the service account in AppViewX.
azure_hub_url	URL of the Azure IoT Hub for communication with devices. Ensure to replace the device number with %s before entering the `azurehuburl`.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for the APIconfig File (continued)

Field	Description
	Sample Input URL - "*https://AzureIotHubTrialSample.azure-devices.net/devices/**%s**?api-version=2021-04-12*"
azure_hub_key	Primary or secondary key of the Azure IoT Hub policy.
azure_hub_policy_name	Name of the policy in Azure IoT Hub (e.g., `iothubowner`).
azure_token_validity	Time duration (in seconds) during which the SAS token remains valid.
certFolder	Path to the folder where issued certificates are stored —**IssuedCerts** folder
backupFolder	Path to the folder where backup certificates are stored.
poll_count	Number of times the standalone server polls the Azure IoT hub's update status, when updating through AppViewX. **Default value**: 5
poll_interval	Time interval (in seconds) between each poll attempt made by the standalone server. **Default value**: 5
update_azure_iot_hub_from_standalone_server	Boolean flag to control whether the Azure IoT Hub update is triggered directly from the standalone server. If set to **false**, the update is handled by AppViewX.
Note: To ensure AppViewX manages the Azure update process correctly, see Configuration for Azure IoT hub in AppviewX.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

config File Configuration

Sample Configuration:

```
{
  "intermediate_cert_config": {
     "common_name": "<Intermediate-Cert-Common-Name>",
     "country": "<Intermediate-Cert-Country>",
     "province": "<Intermediate-Cert-province>",
     "locality": "<Intermediate-Cert-locality>",
     "organization": "<Intermediate-Cert-Organization-Name>",
    "organizational_unit": "<Intermediate-Cert-Organization-Unit-Name>",
     "use_est": true,
     "mtls_auth_cert_path": "<MTLS-Auth-Cert-Path>",
     "mtls_auth_key_path": "<MTLS-Auth-Key-Path>",
     "est_url": "<EST-Agent-Setting-Endpoint-URL>"
  },
  "device_cert_config": {
     "is_device_cert_required": false,
     "common_name": "<Device-Cert-Common-Name>",
     "country": "<Device-Cert-Country>",
     "province": "<Device-Cert-province>",
     "locality": "<Device-Cert-locality>",
     "organization": "<Device-Cert-Organization-Name>",
     "organizational_unit": "<Device-Cert-Organizational-Unit-Name>",
     "mtls_auth_cert_path": "<MTLS-Auth-Cert-Path>",
     "mtls_auth_key_path": "<MTLS-Auth-Key-Path>",
     "est_url": "<EST-Agent-Setting-Endpoint-URL>"
  },
  "new_intermediate_cert": false,
  "mtls_ca_cert": "<CA certificate path to establish MTLS connection>",
  "mtls_server_cert": "<Server certificate path to spin the server>",
  "mtls_server_key": "<Server certificate key to spin the server>",
  "pkcs11_library": "<pkcs11 .so file path>",
  "pkcs11_library_pin": "<pkcs11 library pin>",
  "port": <EST-Port the client listens>,
  "intermediate_private_key_label_in_pkcs11":"<Private key label inside pkcs11 [HSM/TPM]>",
  "intermediate_cert_path": "<Intermediate certificate path>",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"end_certificate_config_1": {
    "end_point_name": "device",
    "extended_key_usage_list": [
        "1.3.6.1.5.5.7.3.1",
        "1.3.6.1.5.5.7.3.2",
        "1.2.3.4.5.6.7.8.9"
    ],
    "is_ca": true,
    "path_length_constraint": 10,
    "validity_in_days": 30,
    "key_usage": {
        "digital_signature": false,
        "decipher_only": false,
        "non_repudiation": false,
        "key_encipherment": false,
        "data_encipherment": false,
        "key_agreement": true,
        "key_cert_sign": true,
        "crl_sign": true,
        "encipher_only": true
    },
    "is_device_cert": true,
    "is_unlimited_validity": false
},
"end_certificate_config_2": {
    "end_point_name": "user",
    "validity_in_days": 31,
    "extended_key_usage_list": [
        "1.3.6.1.5.5.7.3.1"
    ],
    "key_usage": {
        "digital_signature": false,
        "decipher_only": false,
        "non_repudiation": false,
        "key_encipherment": true,
        "data_encipherment": false,
        "key_agreement": true,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "key_cert_sign": false,
            "crl_sign": true,
            "encipher_only": false
        },
        "is_device_cert": true,
        "is_unlimited_validity": false,
        "is_ca": false,
        "path_length_constraint": null
    },
    "end_certificate_config_3": {
        "end_point_name": "other",
        "validity_in_days": 62,
        "extended_key_usage_list": [
            "1.3.6.1.5.5.7.3.1",
            "1.3.6.1.5.5.7.3.2"
        ],
        "key_usage": {
            "digital_signature": true,
            "decipher_only": true,
            "non_repudiation": true,
            "key_encipherment": true,
            "data_encipherment": true,
            "key_agreement": true,
            "key_cert_sign": true,
            "crl_sign": true,
            "encipher_only": true
        },
        "is_device_cert": false,
        "is_unlimited_validity": false,
        "is_ca": false,
        "path_length_constraint": null
    },
    "encryption_key_file_path": "<Credential Encryption Key File Path>"
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Intermediate and Device Certificate Configuration

Field	Description
Intermediate certificate configuration - intermediate_cert_config	
common_name	Common Name (CN) of the Intermediate Certificate.
country	Country associated with the Intermediate Certificate (typically a 2-letter ISO code).
province	Province or state associated with the Intermediate Certificate.
locality	Locality or city associated with the Intermediate Certificate.
organization	Organization name associated with the Intermediate Certificate.
organizational_unit	Organization unit associated with the Intermediate Certificate.
mtls_auth_cert_path	MTLS certificate used for authentication of the Intermediate Certificate issuance. **Note: Intermediate** certificate template must be chosen in the AppViewX EST agent setting.
mtls_auth_key_path	MTLS key used for authentication of the Intermediate Certificate issuance.
est_url	EST Agent URL from AppViewX agent setting for Intermediate Certificate issuance.
use_est	A boolean value (true or false) indicating whether to enroll intermediate certificates using EST protocol or using create certificate API.
Device certificate configuration- device_cert_config	
is_device_cert_required	A boolean value (true or false) to determine if control the configuration of device certificate should be enrolled.
common_name	Common Name (CN) of the Device Certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Intermediate and Device Certificate Configuration (continued)

Field	Description
country	Country associated with the Device Certificate (typically a 2-letter ISO code).
province	Province or state associated with the Device Certificate.
locality	Locality or city associated with the Device Certificate.
organization	Organization name associated with the Device Certificate.
organizational_unit	Organization unit associated with the Device Certificate.
mtls_auth_cert_path	MTLS certificate used for authentication of the Device Certificate issuance.
mtls_auth_key_path	MTLS key used for authentication of the Device Certificate issuance.
est_url	EST Agent URL from AppViewX agent setting for Device Certificate issuance.
new_intermediate_cert: A boolean value (true or false) indicating whether to create a new Intermediate Certificate using AppViewX PKIaas CA.	

Field Description for EST Server Configuration Fields

Field	Description
mtls_ca_cert	Specifies the path to the CA certificate of the client certificate's issuer or root CA, required for establishing a Mutual TLS (mTLS) connection. This may be a single CA certificate or a bundle of intermediate and root certificates associated with the EST client certificate, used to validate the mTLS connection.
mtls_server_cert	Path to the server certificate for spinning up the server in an mTLS environment (**.crt**).
mtls_server_key	Path to the server certificate key for spinning up the server in an mTLS environment (**.key**).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for EST Server Configuration Fields (continued)

Field	Description
pkcs11_library	Path to the PKCS#11 shared library (**.so** file) used for Hardware Security Module (HSM) or Trusted Platform Module (TPM) integration.
pkcs11_library_pin	PIN used to authenticate to the PKCS#11 library (HSM/ TPM).
port	Port number on which the EST (Enrollment over Secure Transport) client listens.
intermediate_private_key_label_in_pkcs11	Label of the private key stored inside the PKCS#11 module (HSM/TPM).
intermediate_cert_path	Path where the intermediate certificate is stored which can be used to issue certificate without fetching a new certificate from AppViewX. **Note:** Pass the `private_key_label` and set the `new_intermediate_cert` field as **false** before proceeding with this option.
Attention: Each **end_certificate_config** block defines the parameters for generating an end certificate, including validity, key usage, and extended key usage (EKU).	

Field Description for Endpoint Configuration

Field	Description
end_point_name	Name of the endpoint receiving the certificate.
validity_in_days	Number of days the certificate will remain valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Endpoint Configuration (continued)

Field	Description
extended_key_usage_list	A list of OID strings representing extended key usages (EKU), such as • `1.3.6.1.5.5.7.3.1` for TLS Web Server Authentication. • `1.3.6.1.5.5.7.3.2` for TLS Web Client Authentication.
key_usage	Boolean flags to specify the certificate's key usages (set true or false for each if required): • **digital_signature**: Allows the certificate to verify digital signatures. • **non_repudiation**: Ensures proof of origin and prevents denial of actions • **key_encipherment**: Enables encryption of keys. • **data_encipherment**: Enables direct encryption of user data. • **key_agreement**: Supports key exchange protocols • **key_cert_sign**: Allows the certificate to sign other certificates. • **crl_sign**: Allows the certificate to sign Certificate Revocation Lists (CRL) • **encipher_only**: Restricts key agreement usage to encryption only. • **decipher_only**: Restricts key agreement usage to decryption only.
is_device_cert	If the value is set to **true** then the device is registered in Azure IoT Hub. Default value is **false**.
is_unlimited_validity	If the flag is set to **true**, the validity is fixed at 31/12/9999, regardless of the `validity_in_days` value. Default value is **false**.
is_ca	If flag is set to **true**, the certificate acts as a Certificate Authority (CA) and the Basic Constraint is set as true.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Description for Endpoint Configuration (continued)

Field	Description
	Default value is **false**.
path_length_constraint	If a value is set, it defines the maximum number of subordinate CAs allowed under this CA. Default value is **Nil** (i.e. unlimited).
encryption_key_file_path	(*Optional*) This parameter specifies the location where a randomly generated encryption key is to be stored. This key is created during the EST server's initial run and is essential for encrypting sensitive information such as the Azure API Key, service account secret, and the PKCS11 pin. The same key is used for both, encryption and decryption operations. **Note:** If this encryption key is deleted, decryption of the previously encrypted data is not possible. Therefore, it is crucial to store this key in a secure location.

Configuring Azure IoT Hub in AppViewX

Creating a Service Account

Service account is required for API authentication with AppViewX.

1. Log in to the AppViewX with valid credentials.
2. Got to (**Menu**) > **Platform** > **IDENTITY** > **Service Account**.
3. Add a new account, by providing the necessary details.
4. Assign the user group to Admin.

Uploading and Enabling the Workflow

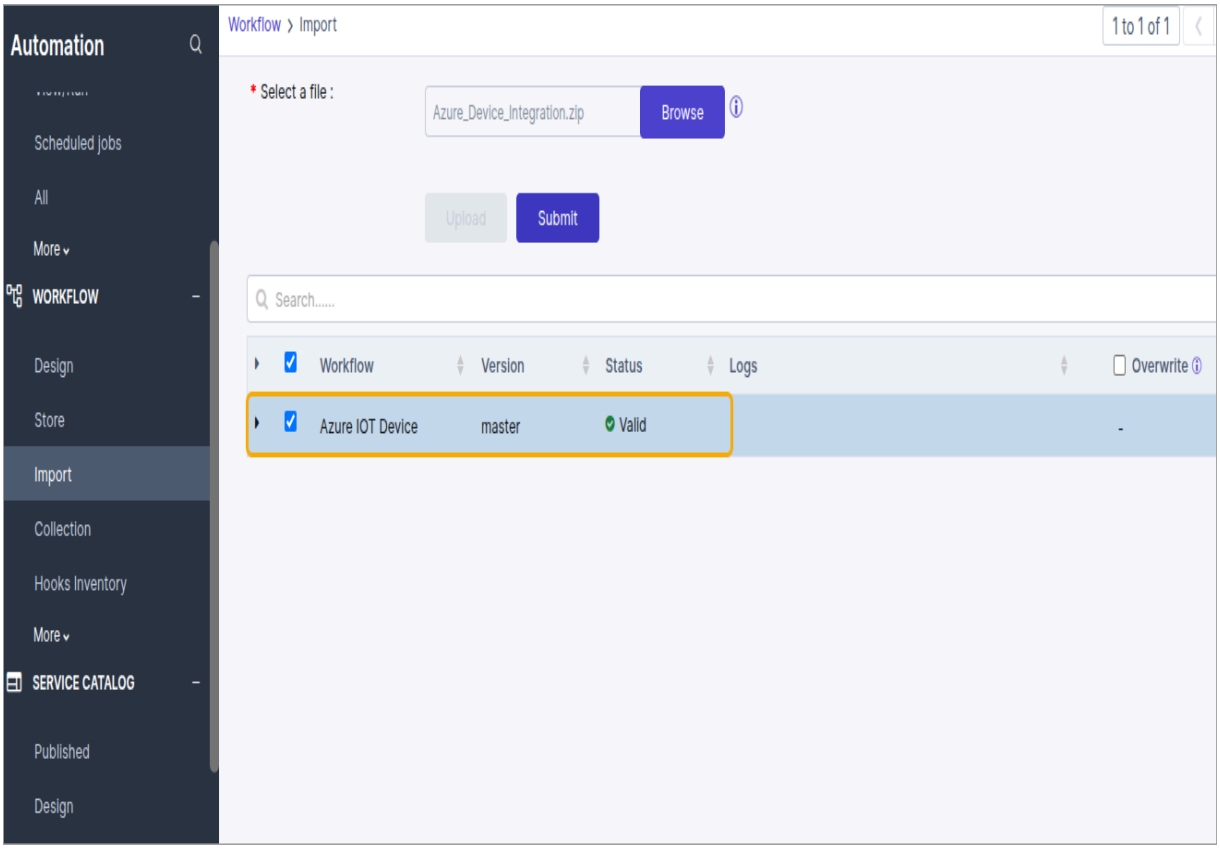
Prerequisites: Download and extract the **EST_STANDALONE_SERVER** file. The extracted file contains the following:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Folders—***Est server*** and ***workflow***
- PDF—***Config Guide***
- text file—***readme***

AppViewX features a workflow that enables registration to the Azure IoT Hub.

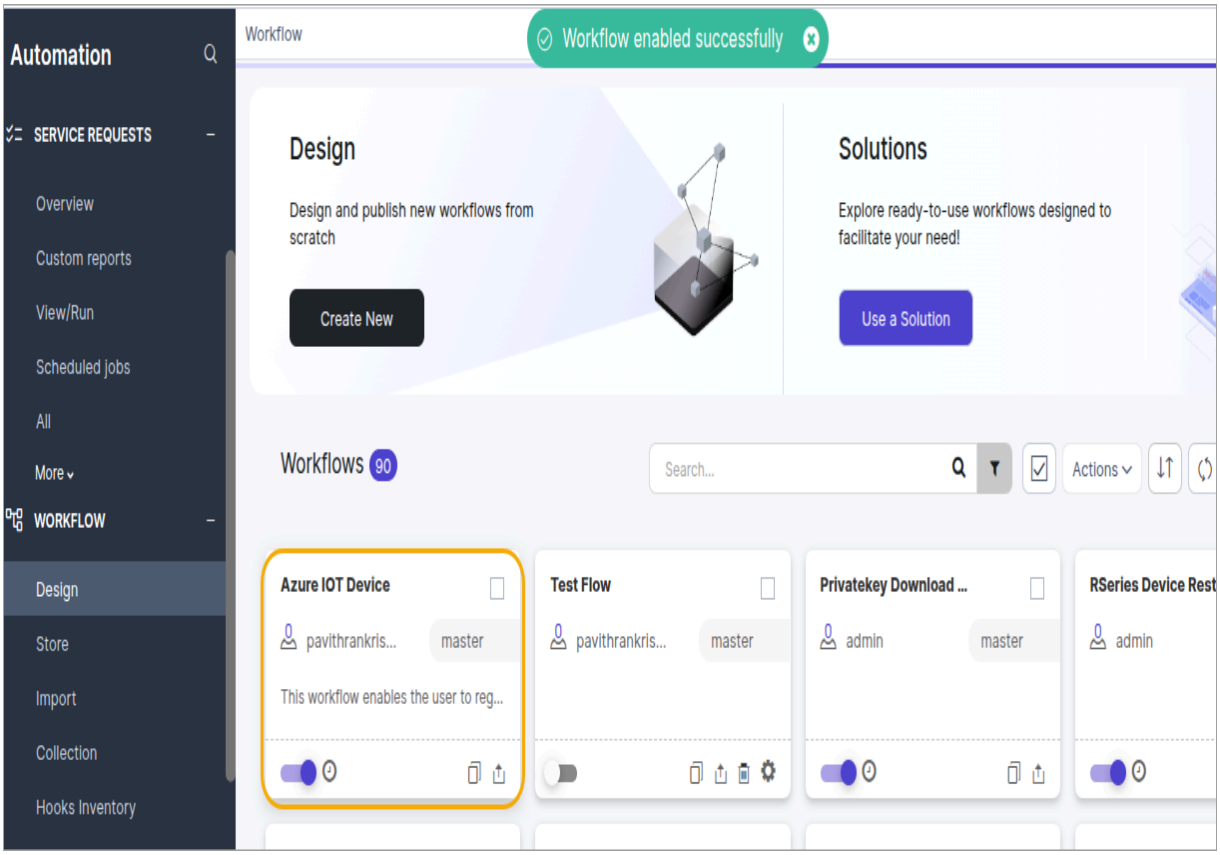
1. Log in to the AppViewX with valid credentials.
2. Got to (**Menu**) > **Automation** > **Workflow** > **Service Account**.
3. Click **Browse**, to upload the provided workflow file [zip file inside the ***workflow*** directory (refer Prerequisites).]
4. Select the uploaded workflow and click **Submit** as shown below.



5. Once submitted, go to the **Workflow** > **Design**, and choose the workflow named **Azure IoT Device**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

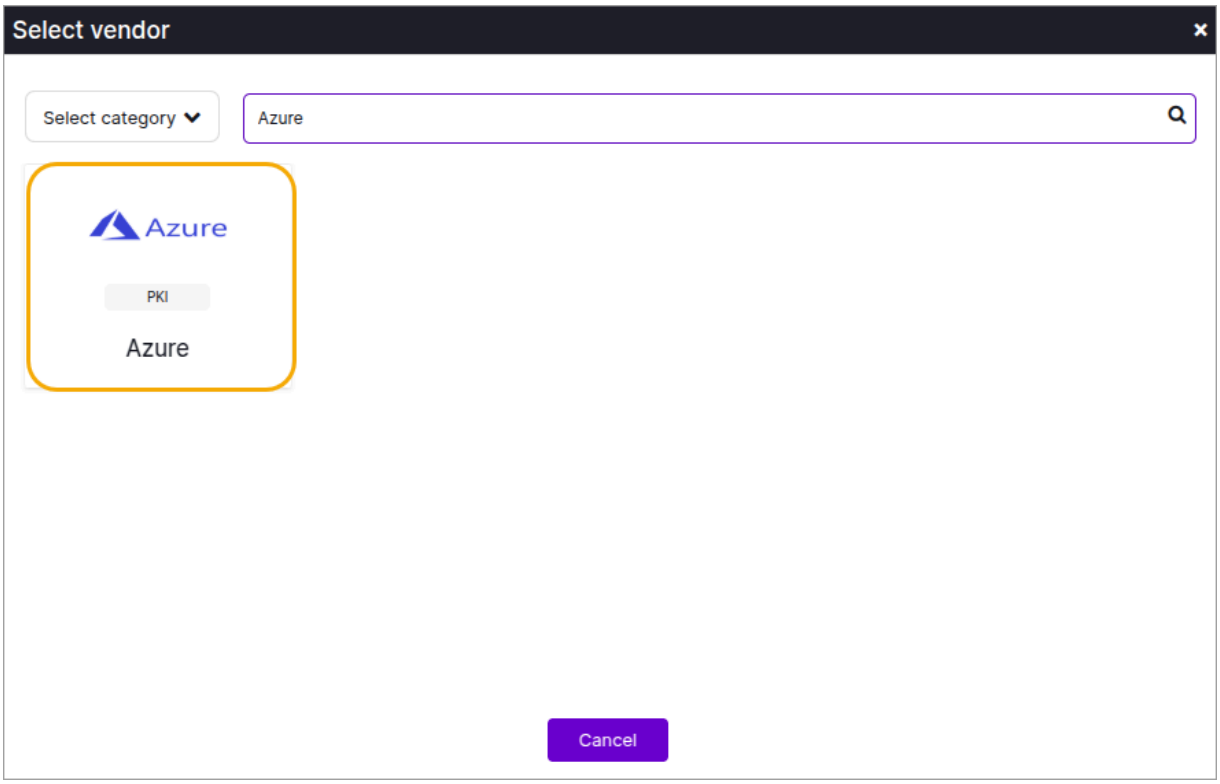
6. Enable the workflow as shown below by clicking on the toggle.



Updating Azure IoT Hub Configuration in AppViewX

1. Log in to the AppViewX with valid credentials.
2. Got to (**Menu**) > **Platform** > **Asset Management** > **Integration Hub**.
3. Click **Add new vendor** icon.
   The **Select vendor** pop-up is displayed.
4. In the **Select vendor** pop-up, enter **Azure** in the search bar.
   The **Azure** vendor icon is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



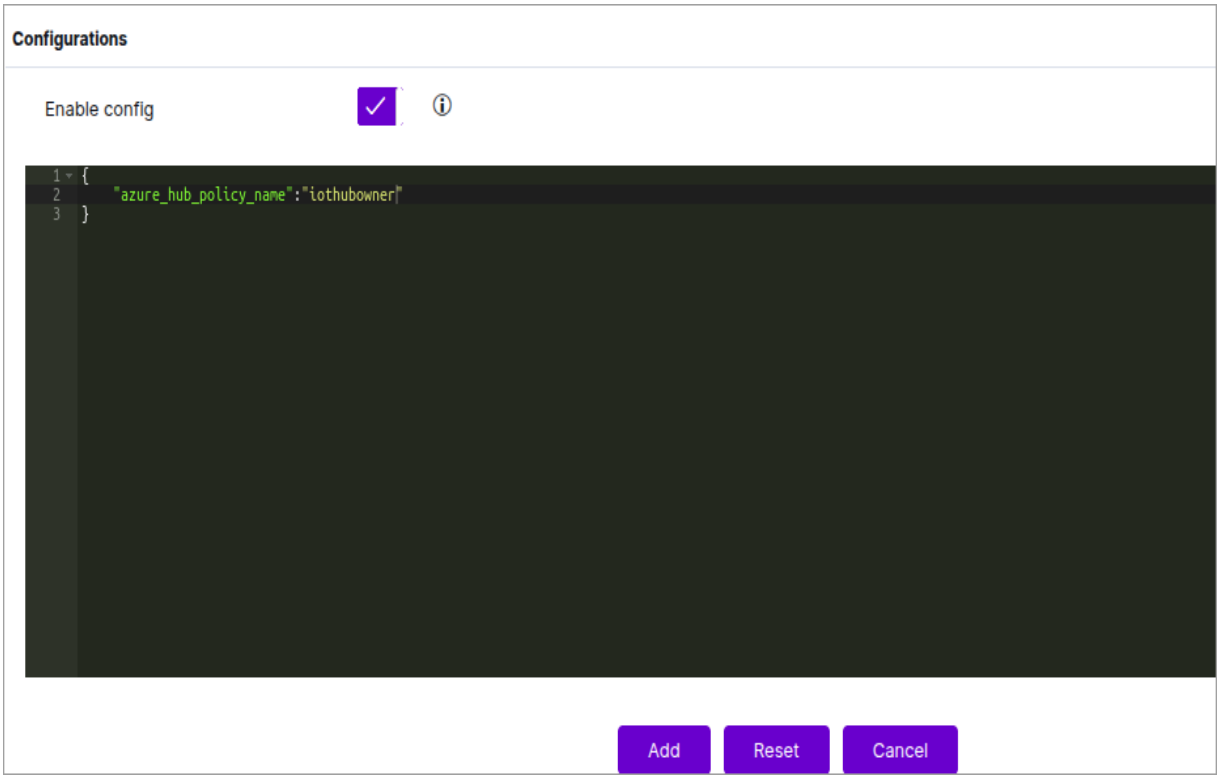
5. Select the **Azure** vendor and enter the following values in the fields specified below:

Field	Value
Name	Enter the value **AzureIoT**.
Datacenter	Select the required value through which the cloud connector device registration/update call should be communicated.
Auth Type	Select **API Key**.
URL	Enter the Azure IOT HUB URL.
Key	Enter the value as **X-Authorization**.
Value	Enter the secret key of Azure IOT Hub.

Enable config	Click the toggle button to enable it and enter the Azure IOT Hub policy name in the config field using the format below:
	`{`
	`"azure_hub_policy_name": "<AZURE_IOT_HUB_POLICY_NAME>"`
	`}`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Value
	Refer figure below.



6. Click **Add** to save the values.

ACME

What is ACME?

ACME, or Automated Certificate Management Environment, is a communications protocol that leverages an agent to automate the process of CSR generation and certificate/key rotation. It is primarily used by the popular public CA, Let's Encrypt, to issue and renew 90-day Domain Validated certificates quickly and efficiently.

The protocol, developed by Internet Security Research Group (ISRG) for Let's Encrypt to issue x.509 (SSL/TLS) certificates, is now supported by other CAs, PKI vendors, and browsers for issuing various types of certificates.

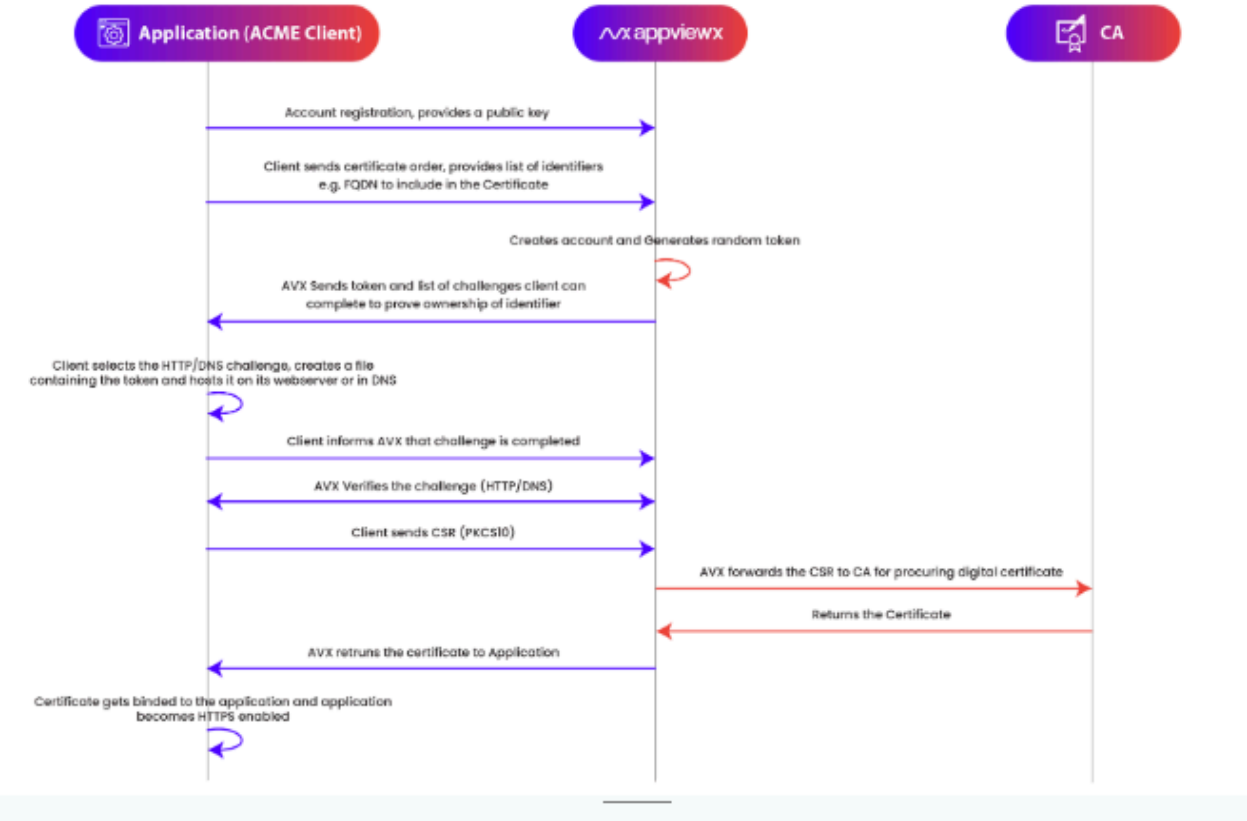
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

ACME is **Automated Certificate Management Environment**, which is a certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire certificates and associated CA certificates. Architecturally, the ACME service (agent) is located between a CA and a client.

- There should be a plugin/pod (avx_vendor_cert_acme_agent) up and running for ACME in AppViewX.
- This ACME plugin works in the HTTPS gateway (The default gateway is used in AppViewX with port 31443)
- It is highly recommended to turn OFF the **Approval Required** flag in **Menu > Inventory > Certificate > Policy** page.
- A valid agent settings should be available in **Menu > Inventory > Certificate > Settings**.

How does ACME work?

This is how ACME works:



1. The application (ACME client) registers an account with AVX and provides a public key.
2. The client sends a request for a certificate, listing the identifiers (e.g., Fully Qualified Domain Names like example.com) to be included in the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. AVX creates the account and generates a random token. It also sends back a list of challenges (like HTTP-01 or DNS-01) to prove the client owns the domain.
4. The client chooses a challenge (e.g., HTTP or DNS), creates a token file and hosts it either on the web server (.well-known/acme-challenge) or in DNS as a TXT record.
5. The client tells AVX that the challenge setup is complete and is ready for verification.
6. AVX accesses the HTTP URL or DNS record to verify the token.
7. The client sends a PKCS#10 CSR (with the public key and requested identifiers) to AVX.
8. AVX forwards the CSR to the CA, which returns a signed digital certificate. AVX sends the certificate back to the application. The application binds the certificate to itself, and HTTPS is enabled.

What's Next?

- Configuring AppViewX ACME Server
- Configuring AppViewX win-acme Client
- Configuring AppViewX Certbot Client
- Configuring AppViewX Posh-ACME Client
- Configuring AppViewX LEGO Client
- Troubleshooting

Configuring AppViewX ACME Server

Prerequisites

On-prem

- Make sure that the following pods are running in the cluster by using the command:

```
kubectl get pods -A | grep acme
```

SaaS

Ensure the https gateway is enabled on the cloud connector while installing it. To do this:

1. Navigate to the installation directory of the cloud connector software.
2. Run

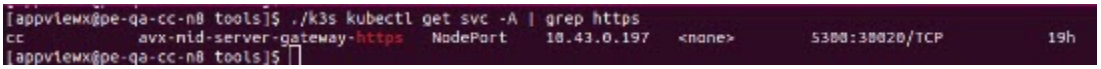
```
cd deps/tools
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Run

```
./k3s kubectl get svc -A | grep https
```

> **Note:** It should have avx-mid-server-gateway-https under namespace cc.



Enabling ACME Services

For On-prem

1. Log onto the AppViewX installer node.
2. Go to </installation_folder/appviewx_kubernetes/scripts> folder.
3. Add the avx-vendor-cert-acme-agent in ENABLED_PLUGINS in the appviewx.conf file.
4. Specify the datacenter (DC) where the gateway must be deployed. avx_vendor_cert_acme_agent=<dc name>

```
ENABLED_PLUGINS=appviewx_dependencies,avx_commons,avx_crontab,avx_config_server,avx_platform_core,avx_platform_amc,avx_platform_q
ueue,avx_platform_gateway,avx_platform_gateway_external,avx_platform_web,avx_subsystems,avx_vendors,avx_subsystems_sync,avx_visua
l_page_builder,avx_vendor_cert_network_discovery,avx_vendor_cert_scep_agent,avx_vendor_cert_intune_agent,avx_vendor_cert_est_agen
t,avx_vendor_cert_acme_agent
SSH_OTHER_USER=appviewx

avx_commons=absecon
avx_config_server=absecon
avx_platform_core=absecon
avx_platform_queue=absecon
avx_subsystems=absecon
avx_subsystems_sync=absecon
avx_vendors=absecon
avx_platform_gateway=absecon
avx_platform_web=absecon
avx_platform_amc=absecon
avx_platform_gateway_external=absecon
avx_visual_page_builder=absecon
avx_vendor_cert_network_discovery=absecon
avx_vendor_cert_scep_agent=absecon
avx_vendor_cert_intune_agent=absecon
avx_vendor_cert_est_agent=absecon
avx_vendor_cert_acme_agent=absecon
```

5. Run the <plugins_install.sh>
6. Verify if ACME is enabled by running kubectl get pods -A | grep acme

For SaaS

HTTPS gateway must be enabled while installing the cloud connector (CC). to do this:

1. Log onto the cloud connector installed node.
2. Go to cc_installed_path/deps/properties.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Open appviewx.properties and set the following fields as *true:*
   a. AUTO_ENROLL_ENABLED=true
   b. ENABLE_MTLS_PROFILE=true
   c. ENABLE_HTTP_PROFILE=true
   d. ENABLE_HTTPS_PROFILE=true
4. Scale down the avx-mid-server-platform pod.
5. Restart the avx-mid-server-starter pod.

> **Note:** Ensure that avx-mid-server-gateway-https is present under namespace cc.

Configuring ACME Server

1. Log on to the **AppViewX** application with valid credentials.
2. Click (**Menu**) > **CERT+** > **Administration** > **Auto Enrollment** > **ACME**.
   The **Auto Enrollment : ACME** page appears.
3. Click the **+ Add** button.
4. Enter the following fields:

Field description on Auto Enrollment : ACME page

Field	Description
Endpoint Details	
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	**For On-prem** • Enter the FQDN address of the AppViewX ACME gateway. It must be the same as the web URL's hostname. **For SaaS** **Using On-premises CC:** • **Without load balancer:** Must be the FQDN of the cloud connector where the auto-enrollment gateway is running. • **With load balancer:** Must be the FQDN of the load balancer.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Using Direct Gateway • In the SaaS setup, to use the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is **<tenant>-aep.<domainname>**.
***Port**	**For On-prem** • By default, it is port 31443. Leave it as is. **For SaaS** **Using On-premises CC** • **Without load balancer:** By default, it is port 30020. Leave it as is. • **With load balancer:** Port must be the listening port of the load balancer. **Note:** • It is recommended to set the listening port as 30020, which is the same as AppViewX. • If the load balancer's listening port is different from 30020, then update the respective port. **Using Direct Gateway** • In the SaaS setup, to use the direct AEP gateway without installing the cloud connector, use port 443.
***Challenge Type**	**Select any of the following:** • **HTTP:** By default, this is selected. • **DNS**
***HTTP Challenge Port**	Specify the port number used for HTTP challenge validation. By default, it is 80. Specify a different port (1 to 65535), if required. Audit logs are available for this under **Alerts & Logs > Certificate Logs.**
***Challenge Validation Type**	**Note:** Only win-acme and Certbot enrollments and re-enrollments use these fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field appears when Challenge Type = DNS. Select any of the following: • **Default:** Select this option to update the DNS TXT record. Access is required to update the record in the DNS server as part of this process. • **DNS Challenge:** Select this option for AppViewX to update the TXT record on the DNS server. AppViewX will require credentials for the DNS server. **Attention:** On clicking DNS Challenge, make sure to onboard your DNS server in the Integration Hub to update the challenge token and to allow addition/modification/deletion of the TXT record. • **Enterprise secure challenge:** Select this option for validation to happen based on the A record of the domain. **Note:** The options **DNS Challenge** and **Enterprise Secure Challenge** are supported only in appviewx provided ACME clients. For all the open source clients always use the **Default option**
***Validation Method**	This field appears when Challenge Validation Type = Enterprise secure challenge. Select any of the following: • **Secure:** This method performs strict validation of the client's IP address against the existing A record of the domain. • **Any:** The client's IP must be part of one of the available A records for the domain. • **Ignore:** Select this option for domains that have been pre-validated.
Validate HTTP Challenge via Proxy	This field appears when Challenge Type = HTTP. If enabled, the communication with the ACME client to fetch the HTTP challenge token is via the proxy details provided in the **General Settings**.
***Allowed Domain Names**	This is a mandatory field if you have chosen Challenge Validation Type as DNS Challenge or Enterprise secure challenge. You can provide multiple domain names separated by a comma.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

Load Balancer Configuration

It is recommended to set the listening port as 30020, which is the same as AppViewX.

Health check URL for load balancer:

a. **HTTP method:** GET
b. **Healthcheck API:** https://<hostname>:30020/
   i. **Hostname:** Hostname of cloud connector enabled with the MTLS gateway.
   ii. **Expected response code:** 404. As the load balancer is accessing the URL without any parameters, it will receive a 404 response.

Field description of Add New Vendor page on Integration Hub page

Field	Description
***Category**	This field is pre-populated on selecting **Select Category** as **IOT**.
***Vendor**	This field is pre-populated on selecting **Infoblox**.
***Name**	Enter a name.
Version	Provide a version, if required.
Description	Provide a description, if required.
Upload Image	Upload vendor image.
Tags	Provide tags.
Data center	Select a data center from the dropdown list.
Credentials	
Type	Select between REST or SSH. By default, REST is selected.
Auth Type	Select a value from the dropdown list. By default, Basic Auth is selected.
***URL**	Enter the URL and validate it by clicking **Validate URL.**
***Credential Type**	By default, Manual entry is selected. Keep the selection as is.
***Username**	Enter the assigned username. (This field is displayed for Manual entry only.)
***Password**	Enter the password.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Configurations	
Enable config	By default, this toggle button is disabled. Enable it to add another vendor configurations/attributes in JSON format. Attributes can be referred to as variables in workflow automation.
***:** mandatory fields	

Field description in CA Accounts section

Field	Description
***Certificate Group**	Select a specific group under which certificate needs to be enrolled.
***Select CA**	Select the required CA from the available options. The certificate will be enrolled under the selected CA. The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS • AppViewX PKIaaS Native • Amazon Private CA • DigiCert • DigiCert One • EJBCA • Entrust • Entrust MPKI • GlobalSign SSL • GlobalSign Atlas • GlobalSign MSSL • Google • HydrantID • IDnomic • LetsEncrypt • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust • Sectigo (Comodo Certificate Manager) • SwissSign

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The Vendor Specific Details and Custom Attributes section are displayed for some of the CAs as follows: • DigiCert • Ejbca • Entrust • Entrust MPKI • GlobalSign MSSL • MS Enterprise • Nexus
*: mandatory fields	

Note: Use the port number that appears when you enable ACME services.

When **AppViewX** is selected as CA, the fields for AppViewX CA are as follows:

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with the ACME client machine.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: Mandatory fields	

When **AppViewX PKIaaS Native** is selected as CA, the fields for AppViewX PKIaaS Native are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for AppViewX PKIaaS Native - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Template Name	Select a template name from the dropdown list.
***Issuer Name**	Select an issuer name to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. **Note:** For some CAs, the validity available in their respective CA portal is considered despite the specified certificate validity.
*: mandatory fields	

When **Amazon Private CA** is selected as CA. The fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the group's associated policy. Select an appropriate value as required.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields	

When **AppViewX PKIaaS** is selected as CA, the fields for AppViewX PKIaaS CA are as follows:

Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with the ACME client machine.
***Issuer Location**	Select the issuer location associated with the CA account.
***Issuer Name**	Select a valid issuer associated with the CA account.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields	

When **DigiCert** is selected as CA. The fields for DigiCert CA are as follows:

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Division**	Select a division associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Certificate Type**	Select a valid certificate type associated with the CA account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The dropdown is populated with the first available value. Select an appropriate value as required.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Order Validity**	Validity of the certificate to be enrolled.
*: mandatory fields	

If the **Select CA =DigiCert**, then a separate section **Vendor Specific Details** is displayed after the CA Accounts section with two fields described below.

Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type. The dropdown is populated with the first available value. Select an appropriate value as required.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with the account balance. Returns an error if this option is disabled for the account or if the account has an insufficient fund. • **Bill To Default Credit Card** - Pay with the account's default credit card. Returns an error if no default credit card is configured for the account
*: mandatory fields	

When **DigiCert One** is selected as CA. The fields for DigiCert CA are as follows:

Details for DigiCert One CA - Field Description Table

Fields	Description
***CA Account Name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server or Client.
Proxy Required	Enable this field if the CA communication needs to happen via proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center for CA communication, with the CC node being the recommended option. The selected node will handle the communication through the chosen CC node.
CA Configuration	
***Base URL**	This URL will contain the hostname of the DigiCert CA instance and used for constructing the API requests.
***Authentication method**	By default, API Token is selected.
***API Token**	Enter the API token to authorize the communication between AppViewX and DigiCert One.
Allow Seat ID during enrollment	Enabling this field displays a Seat ID field in the Auto enrollment settings that you can use instead of the CA settings.
***Seat ID**	Unique value assigned to identify an entity in the DigiCert One account.You can provide multiple ID separated by a comma. They can be used for enrollment, renewal, and regeneration.
Use DigiCert One to switch certificates from DigiCert MPKI	Enable this field to automatically switch your DigiCert MPKI certificates to DigiCert One with auto-enrollment/auto-regenerate.
*****: mandatory fields	

When **EJBCA** is selected as CA. The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: mandatory fields	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
*: mandatory fields	

When **Entrust** is selected as CA. The fields for Entrust CA are as follows:

Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select a valid certificate type associated with the CA account. • If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. • If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the requester name.
Requester Email	Enter a valid email ID.
Requester Phone	Enter the 10-digit phone number.
***: mandatory fields	

When **Entrust MPKI** is selected as CA. The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***: mandatory fields	

If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Certificate Profile**	Select a certificate profile from the dropdown list.
***: mandatory fields	

When **GlobalSign (GlobalSign SSL)** is selected as CA. The fields for GlobalSign (GlobalSign SSL) CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for GlobalSign SSL CA - Field Description Table

Fields	Description
***CA Account**	A unique name to identify the CA setting. No special characters other than '.', '-','_' are allowed. The name should not start with special characters.
***Certificate Type**	Certificate Type for which CLM actions will be enabled. Select a value from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

If the selected CA is GlobalSign (GlobalSign SSL), a separate section **Vendor Specific Details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for GlobalSign (GlobalSign SSL) CA - Field Description Table

Fields	Description
***Domain Admin CA Name**	Select a CA name from the dropdown list.
*: mandatory fields	

The following field is displayed in the **Point of Contact** section as per the selected CA if the **Select CA =GlobalSign**, and the **Certificate type = Organization SSL**. The CA mandates the point of contact information (**First Name**) for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.

When **GlobalSignMSSL** is selected as CA. The fields for GlobalSign MSSL CA are as follows:

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled (in days/months/years).
***:** mandatory fields	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
***:** mandatory fields	

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
***:** mandatory fields	

When **GlobalSignAtlas** is selected as CA. The fields for GlobalSign MSSL CA are as follows:

Details for GlobalSignAtlas CA - Field Description Table

Fields	Description
***API Credential Friendly name**	select the user-defined label in AppViewX that identifies and maps the API credentials used for authenticating with the GlobalSign Atlas CA.
***Certificate Profile**	Select a certificate profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: mandatory fields	

Note: The **Generic Fields** section will be displayed for this CA, with fields such as *organization*, *organizational_unit*, *country*, *state*, *locality* etc, as configured in the Certificate Authority settings.

When **Google** is selected as CA. The fields for Google CA are as follows:

Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
Template Name	Select a template name from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields	

When **HydrantID** is selected as CA. The fields for HydrantID CA are as follows:

Details for HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

When **IDnomic** is selected as CA. The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

When **LetsEncrypt** is selected as CA. The fields for Let's Encrypt CA are as follows:

Details for LetsEncrypt CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields	

When **Microsoft Enterprise** is selected as CA. The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields	

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed with a **Template Name** dropdown after the CA Accounts section.

When **Microsoft Standalone** is selected as CA. The fields for Microsoft Standalone CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields	

When **Nexus** is selected as CA. The fields for Nexus CA are as follows:

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor Specific Details - Field Description Table

Fields	Description
***Procedure**	Select the procedure based on the configurations made in the Certificate Authority Setting.

When **OpenTrust** is selected as CA. The fields for OpenTrust CA are as follows:

Details for OpenTrust CA - Field Description Table

Fields	Description
***CA Account name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Management Profile**	Select the certificate issuance policy defined in OpenTrust CA.
Zone	The AppViewX configuration wrapper that maps to a CA + profile, and is used by end-users or automation to request certificates consistently.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields	

When **Sectigo (Comodo Certificate Manager)** is selected as CA. The fields for Sectigo (Comodo Certificate Manager) CA are as follows:

Details for Sectigo (Comodo Certificate Manager) CA - Field Description Table

Fields	Description
***CA Account**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Certificate Type**	Select a value from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

When **SwissSign** is selected as CA. The fields for SwissSign CA are as follows:

Details for SwissSign CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate creation operations.
***Client Name**	Select the specific client.
***Product**	Select the specific product.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*****: mandatory fields	

5. Configure the **Advanced Settings** details as follows:
   The following table provides the field description for Advanced Settings:

Advanced Settings - Field Description Table

Fields	Description
***Fetch Certificate Parameters**	Select *Yes* or *No*. Setting the radio button to *Yes* enables the system to automatically fetch certificate parameters from a Suggestive Policy and append them to the client CSRs.
***Restrict Revocation**	This option restricts the revocation of certificates through this endpoint. • If it is set to No, then the certificates are revoked through the ACME endpoint. • If this is set to Yes, then the certificates cannot be revoked through the ACME end point.
***Restrict Wild Card Certificate**	This option restricts the issuance of wildcard certificates through this endpoint. The default value is set to “No”. • If it is set to No, then wildcard certificates are issued through the endpoint. There are no restrictions to certificate enrollment through the ACME endpoint. • If this is set to Yes then wildcard certificates are issued through the ACME endpoint. Choosing this option will not allow Common Name or DNS starting with *.
***High Speed Transactions**	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol’s Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR &

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed. • If it is set to **No**, then the AppViewX will do the default behavior of enrolling a new certificate for each request.
Block Duplicate Certificates	By default, this option is disabled. Enable this option to prevent users from requesting duplicate certificates for the same common name from the same device within a defined timeframe. On enabling this option, the following fields are displayed: • ***Max duplicate certificate requests:** You can limit duplicate certificates within a set timeframe. By default, up to 3 duplicates are allowed per hour, with a maximum of 100 duplicates in 240 hours. • ***Block Duration:** By default, this is set to 24h. Value can range between 1 and 240h. For example, if 3 duplicate certificates are blocked for 1 hour at 11:40:03, and 3 matching requests (same CN, SAN, device endpoint, and ACME agent) arrive within that hour, those requests will remain blocked for 24 hours—until 12:40:03 the next day—after which they will be automatically unblocked. During this period, any attempt to enroll certificates with the same common name from the same device will result in an error. **Note:** • If IP forwarding is not enabled (for example, in a loadbalanced environment), all requests may appear to originate from the same IP address. This could potentially cause unexpected behavior when block duplicate requests are enabled. • You can manually unblock the duplicate certificates by clicking Unblock Requests on the ACME Auto Enrollment page.
***Certificate Threshold**	This field is enabled only if Return Existing Certificate = Yes. Enter the number of days in this field. This value is used to Initiate a new

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	certificate request if the certificate is nearing the expiry date i.e., if existing certificate validity is less than the entered value.

***External Account Binding**	The Certificate Authority operating the ACME server needs to provide the ACME client with a MAC Key and a Key Identifier using mechanisms outside of ACME (either through Email/SMS/ downloading or copying from the local login account). The key identifier must be an ASCII String. The MAC key will be provided in base64 URL encoded form to maximize the compatibility between non-ACME provision systems and ACME clients.
	• Select Yes to enable the External Account Binding (EAB). The following fields are enabled:
	  • EAB Algorithm
	  • EAB Generation Logic
	  • MAC Value
	  • Key Identifier
	• Select No to disable the EAB.

EAB Algorithm	This dropdown list contains a list of preset algorithms that generate the MAC Value and the key identifier that are used for enrollment. The values are • HS256 • HS384 • HS512
EAB Generation Logic	This field has two options: Generate Static and Generate Dynamic. • **Generate Static**: Application generates the Key Identifier and MAC Value and displays the same in the respective fields. The MAC Value is displayed with an asterisk (*) symbol and the Key Identifier as plain text. Option to copy the values is provided. • **Generate Dynamic**: These credentials are unique for each user and are shared to the respective email IDs. While creating an account, the EAB credentials are validated against the email ID provided.
MAC Value	The MAC value as generated by the EAB Algorithm
Key Identifier	The Key identifier value as generated by the EAB Algorithm.
When **Generate Dynamic** is selected:	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***EAB Algorithm**	This dropdown list contains a list of preset algorithms that generate the MAC Value and the key identifier that are used for enrollment. The values are: • HS256 • HS384 • HS512
***Configuration Type**	Select the type of configuration as below: • User Group - enabled by default. • CSV - currently disabled • LDAP Group - currently disabled
***User Group List**	A dropdown with a list of available user groups with multi-select option. Select one or more user groups.
*: mandatory fields	

The **Generate Dynamic** option also displays a table with the configured values as follows:

Description for configured values of Generate Dynamic selection

Table Options	Description
User Name	Column to display the user name / user group. A checkbox is available next to the user name to perform actions described below.
Mail Address	Column to display the mail address where the EAB details were sent.
EAB Status	Displays the status as follows • Activated • Deactivated • Credentials not sent
Last Updated Time	Column to display the date and time when the configuration was last updated.
Search	Type the user name/group, mail address, status etc to find or display desired values in the table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Table Options	Description
Actions	The Actions dropdown field has the values below. Select the checkbox next to the user name and then click Actions. • **Activate** - Deactivated EAB credentials and ACME accounts are marked as activated. An activation email is sent to the user. • **Deactivate** - EAB details and ACME accounts are marked as deactivated. A deactivation email is sent to the user. • **Rotate** - New EAB credentials will be generated and shared to the user. The ACME accounts - Dynamic and Static, created with existing credentials are deleted. • **Resend** - Existing EAB details are resent to the users through email.

6. Click **Save**.

Verifying ACME Server

To validate the AppViewX configuration:

1. Configure the ACME endpoint in AppViewX GUI.
2. Ensure that the agent configuration must be in **valid** status.

3. If the configuration is completed and the agent status is valid, refresh the ACME URL from the web browser. The expected response should be:

```
{
  "newAuthz": "https://<ip>:<port>/avxapi/test-acme/acme/new-authz",
  "keyChange": "https://<ip>:<port>/avxapi/test-acme/acme/key-change",
  "revokeCert": "https://<ip>:<port>/avxapi/test-acme/acme/revoke-cert",
  "meta": {   "externalAccountRequired": false  },
  "newNonce": "https://<ip>:<port>/avxapi/test-acme/acme/new-nonce",
  "newAccount": "https://<ip>:<port>/avxapi/test-acme/acme/new-account",
  "newOrder": "https://<ip>:<port>/avxapi/test-acme/acme/new-order"
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Binding Custom Certificate to Gateway in Cloud Connector

This section describes the steps to replace the Default TLS Certificate with Signed Certificate in on-premises CC (Cloud Connector).

By default, AppViewX provides a default certificate in the gateway. For ACME, you must bind a valid certificate (Certificate with CC hostname) with the gateway.

To bind a TLS certificate to gateway :

- The certificate's common name must be the hostname of the CC.
- Download the certificate with .crt format and the key file.

To update the certificate:

1. Copy the certificate and the key file to <cc_installation_folder>/deps/properties/ directory.
2. Go to the cc_installation_folder and run:

   ```
   ./avxctl upgrade gateway-cert
   ```

3. You will be prompted with the question, *Do you want to bind a SSL certificate to gateway? (y/n)*:

   a. To bind a certificate to the gateway, enter **y**.

   b. You will then be asked for the *certificate path* and the *key path*. Provide the relative path of the files as indicated:

   If the certificate and key file is copied into <cc_installation_folder>/deps/properties/ folder, then the path should be:
   - *Please enter the certificate file path:* /properties/test.crt
   - *Please enter the key file path:* /properties/test.key

   c. If this step is not required, enter **n**.

4. You will now be prompted with, *Do you want to add trusted CA certificates for mTLS authentication for EST? (y/n):*

   Enter **n** (This step is applicable only for EST protocol).

5. Wait for the script to complete and the gateway will be upgraded.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: When there is a load balancer on top of the cloud connector, then a valid certificate must be bound to the load balancer using the load balancer's hostname.

Best Practices

- **Certificate Group and CA Policy Setup:**
  - Create a dedicated certificate group and CA policy specifically for auto-enrollment in AppViewX.
  - While configuring the policy, ensure only the required key bit-length is selected (minimum: **2048-bit**).
- **Enable SSL Verification:** Always bind a valid SSL certificate on the AppViewX Gateway or Cloud Connector (CC) and enable SSL verification for secure communication.
- **Restrict Domain Issuance:** Use the **Allowed Domain Names** field to limit certificate issuance to specific domains and prevent unintended wildcard certificate issuance by disabling it in the agent setting configuration where necessary.
- **Ensure High Availability:** Deploy a load balancer in front of Cloud Connectors to establish a high-availability setup.
- **Use External Account Binding (EAB):** Implement EAB as an added layer of authentication for enhanced security.

Configuring AppViewX win-acme Client

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Getting Started

Prerequisites

- The AppViewX server/cloud connector (CC) must be bound with a valid certificate. See Section, *Binding Custom Certificate to Gateway in Cloud Connector*.
- The certificate bound to the AppViewX or CC gateway must be trusted by the Windows client machine.
- To trust the certificate, import the root and the issuer certificates to the Windows root and intermediate trust stores.
- A proper DNS entry for the Windows server where winacme is being installed.
- A valid ACME endpoint must be configured on the AppViewX GUI.
- To enable client connections, ensure the following ports are open for inbound communication in AppViewX:
  - 31443 is open for on-premises deployment and port.
  - 30020 in cloud connectors is open for SaaS deployment in AppViewX.
- If the domain validation is set as HTTP, ensure port 80 is accessible on your Windows machine to allow AppViewX to establish a connection.
- If the DNS validation is for DNS challenge, then the DNS server must be up and running and the DNS credentials file should be correctly configured.
- Certificate attributes and custom attributes must be configured to capture the attributes in the AppViewX GUI (if required).

System Requirements

- **Operating System:** Windows Server 2012 R2 SP1 or higher
- **Framework:** .NET Core 5 or higher
- **RAM:** 4GB or higher

Installing win-acme Client

1. Download the latest version from the AppViewX release portal.
2. Unzip files to a non-temporary folder so that the scheduled task can be run.
   We recommend using `%program files%\win-acme`.
   The settings.json file inside the win-acme folder is used for further configurations.

Installing Bluecat Micetro Plug-In

To install Bluecat Micetro plug-in:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to the winacme home directory. Copy the plugin.validation.dns.bluecatmicetro.v25.0.0.0.zip into the winacme home directory.
2. Extract the plugin.validation.dns.bluecatmicetro.v25.0.0.0.zip and ensure that the plugin.validation.dns.bluecatmicetro.v25.0.0.0 folder is available in the winacme home directory.
3. Run the following command:

```
Sample command

./wacs.exe --target manual --validation bluecatmicetro --host  --credentialfilepath --validationmode dns-01 --verbose
```

4. bluecat_credentials_file_format:
   - hostname=
   - username=
   - password=

Configuring win-acme

Configuring URL

1. Go to **Cert+ > Administration > Auto Enrollment > ACME**.
2. Copy the URL from the **Directory URL** field.
3. Update the **DefaultBaseUri** field in the settings.json file.

Enabling Polling

The following configurations are within the **Acme** category in the settings.json file:

- Configure the **RetryCount** parameter to determine the maximum number of times to refresh validation and order status, while waiting for the ACME server to complete its tasks. By default, this value is set to **15**.
- Configure the **RetryInterval** parameter to the amount of time in seconds to wait for each retry. By default, this value is set to **5 seconds**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Example: Let us consider a scenario where the **RetryCount** is set as **15**, and the **RetryInterval** is configured as **5** seconds. In this case, the **total timeout duration (polling time)** is calculated as 15 multiplied by 5 seconds totaling 75 seconds.

Setting Custom and Certificate Attributes

Custom attributes represent fields that are specific to the Certificate Authority (CA). These attributes are transmitted to the CA for processing to serve different purposes in different scenarios.

Certificate attributes are included in the payload sent to AppViewX. They are primarily used internally for categorization and management purposes. These values must be added in the settings.json file.

Both these attributes are optional fields, so they can be left blank.

Example of cert and custom attributes in settings.json file:

"certAttributes" : {"id":"12345678", "manager":"managerName2"},

"customAttributes" : {"email_address":"test@appviewx.com","Director":"Name"}

```
        "organizationUnit" : "IOT",
        "email" : "testavx@appviewx.com"
},
"certAttributes" : {"id":"12345678", "manager":"managerName2"},
"customAttributes" : {"email_address":"test@appviewx.com","Director":"Name"}
}
```

Providing additional CSR Parameters

You can configure the following fields under the existing CSR field in the settings.json file present in the win-acme folder:

- Organization
- Organization unit

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Country
- State
- Locality
- Email-ID

Note: These fields are optional, so they can be left blank. When filled, they are fetched from the settings.json file for certificate renewal and enrollment.

A sample json file is as shown:

Note: You can customize the CSR parameters only in the win-acme provided by AppViewX.

Actions using win-acme

Enrolling Certificates

You can enroll certificates using:

- Interactive terminal -OR-
- PowerShell script

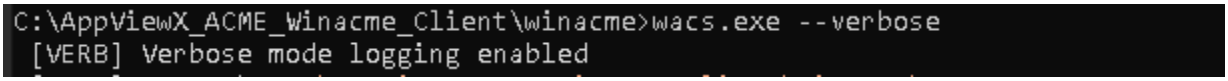
Enrolling Certificates using Interactive Terminal

Prerequisites:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

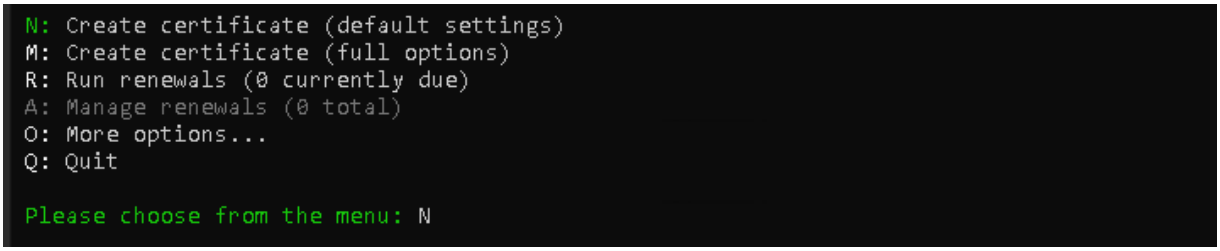
Run the following command with administrator privileges:

```
wacs.exe
```

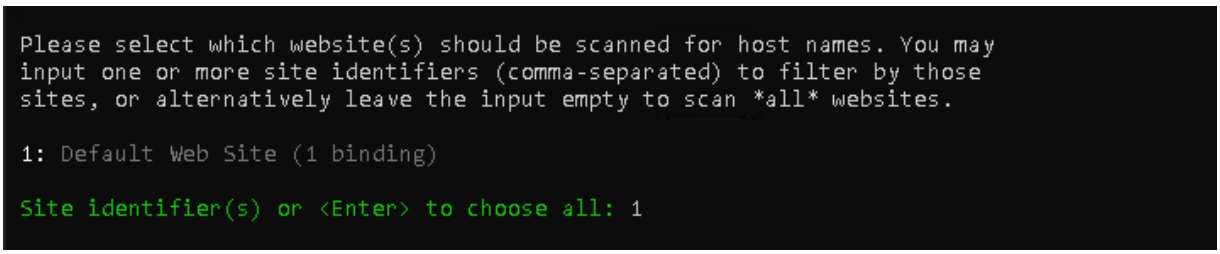


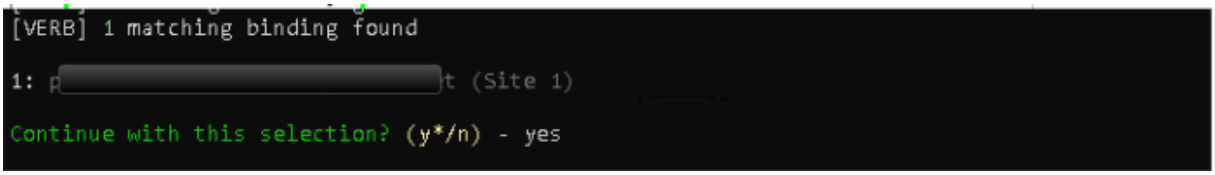
Note: The default settings are for users installing a regular (non-wildcard) certificate on their local IIS instance.

1. To create a new certificate with default settings, choose N from the main menu.



2. Choose how you want to determine the domain name(s) that are to be included in the certificate. This can be derived from the bindings of an IIS site or can be entered manually.



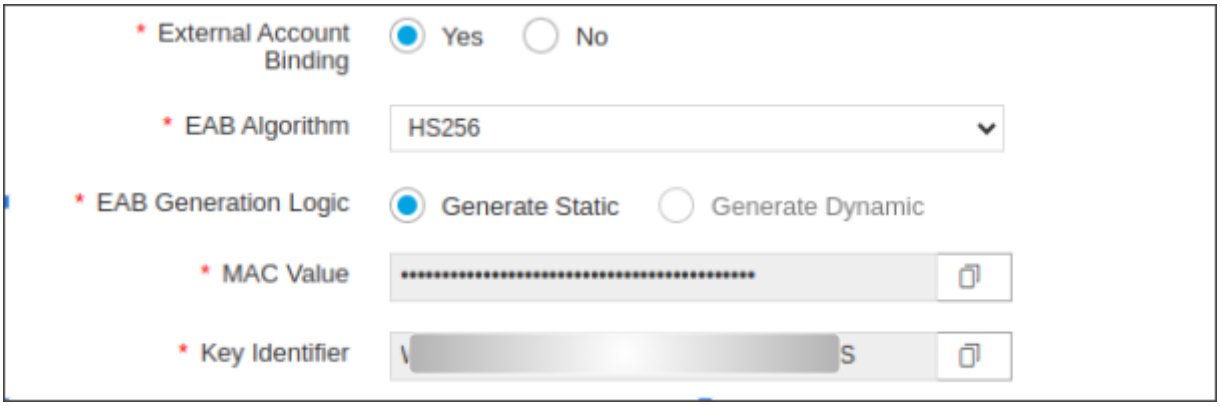


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If EAB is enabled in the AppViewX ACME configuration settings, win-acme will prompt to enter the key identifier and key (base64 url encoded) [enter the value from MAC value in the place of key (base64 url encoded)]

```
Create certificate failed, retry? (y/n*) - yes

This ACME endpoint requires an external account. You will need to provide a
key identifier and a key to proceed. Please refer to the providers
instructions on how to obtain these.

Key identifier: [redacted]

Key (base64url encoded): ****************************************
[testwinacme.appviewx.net] Authorizing...
```

AppViewX ACME configuration:

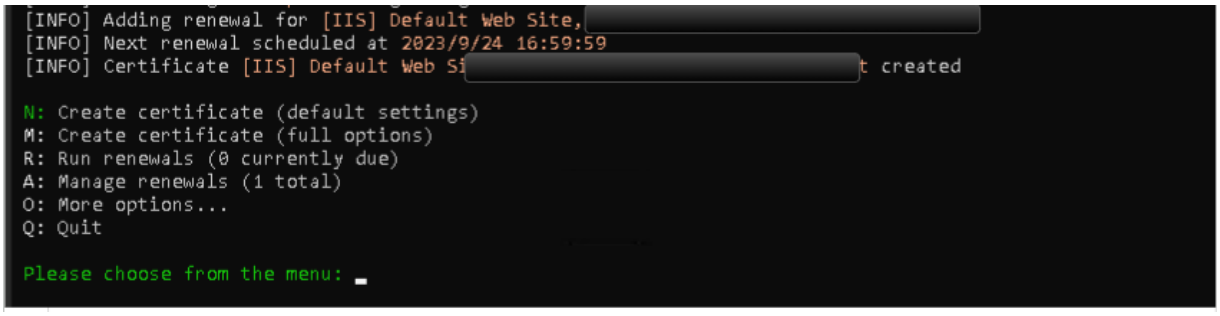


3. A registration is created with the ACME server, if no existing one is found. You will be prompted to agree to its terms of service and to provide an email address that the administrators can use as contact information.

```
[VERB] No account found, creating new one
[VERB] Terms of service downloaded

Enter email(s) for notifications about problems and abuse (comma-separated): <Enter>
```

4. The program communicates with the ACME server to confirm ownership for the certificate you want to create. By default, the http validation mode is used and handled by AppViewX's self-hosting plugin. Getting the validation correct can be the most challenging aspect of obtaining an ACME certificate. If problems persist, refer to the common issues.
5. After the proof has been provided, the program gets a new certificate from the ACME server and creates/updates the IIS bindings as required according to the logic documented here.

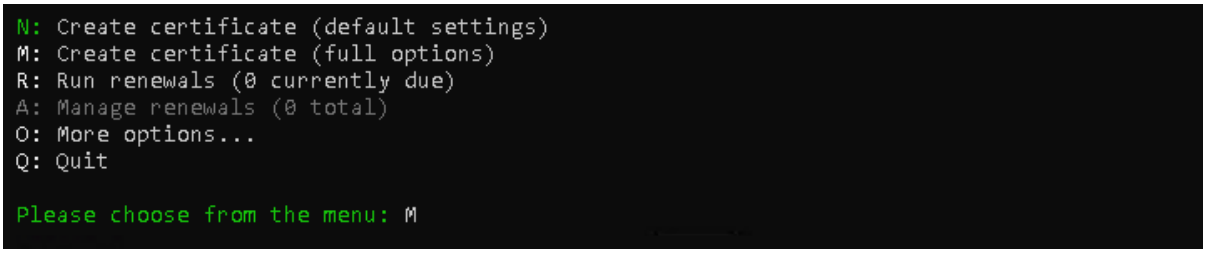
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



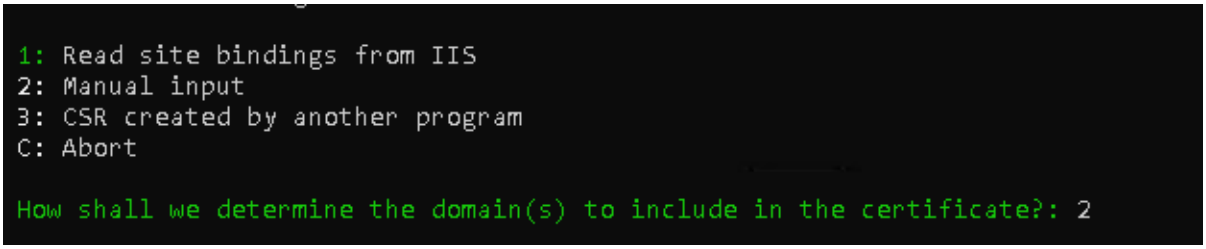
The program stores all choices made while creating the certificate and applies them for each subsequent renewal.

Steps for using *M: create certificates with full option*

1. Choose M to create certificates using full options.



2. Choose 1 to read site bindings from IIS server; else, choose 2 to provide the domain name manually.



3. Continue with the default options for HTTP Challenge validations (The number highlighted in green). HTTP challenge validation is the most common challenge type. ACME server will give a token to the ACME client, and the ACME client puts a file on the web server at http://<YOUR_DOMAIN>/.well-known/acme-challenge/<TOKEN>. Once the token is published in the webserver, AppViewX will send an HTTP request to fetch the token from the client machine.

> **Note:** The common name must be resolving to the client machine IP address and port 80 of the client machine must be accessible by AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
1: [http-01] Save verification files on (network) path
2: [http-01] Serve verification files from memory
3: [http-01] Upload verification files via FTP(S)
4: [http-01] Upload verification files via SSH-FTP
5: [http-01] Upload verification files via WebDav
6: [dns-01] Create verification records manually (auto-renew not possible)
7: [dns-01] Create verification records with acme-dns (https://github.com/joohoi/acme-dns)
8: [dns-01] Create verification records with your own script
9: [tls-alpn-01] Answer TLS verification request from win-acme
C: Abort

How would you like prove ownership for the domain(s)?: 2
```

4. Provide the default option 2 to create the private key for the certificate.

```
1: Elliptic Curve key
2: RSA key
C: Abort

What kind of private key should be used for the certificate?: 2
```

5. To store the certificate in the Windows certificate store, enter 4.

```
1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store
5: No (additional) store steps

How would you like to store the certificate?: 4
```

6. Choose the WebHosting option/ default option to store the certificates in that particular store. (The certificates can be found in the Windows machine certificate store > Web Hosting > Certificates.)

```
1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 3
```

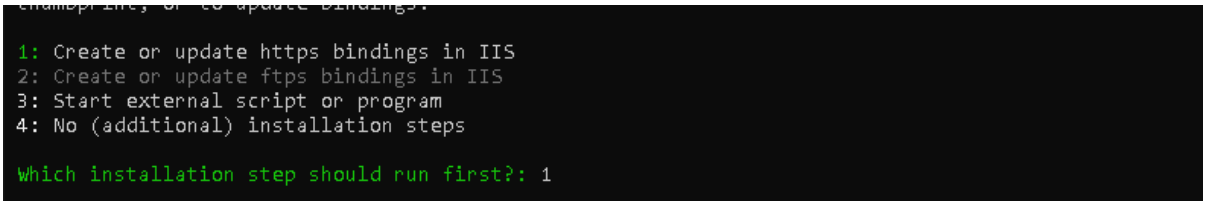
Note: To store the certificate in the personal store use the option **2 instead of 3.**

7. Enter the default option 5 and continue.

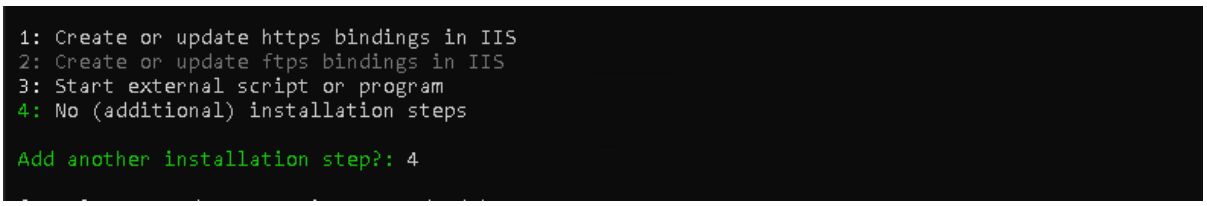
```
1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store
5: No (additional) store steps

Would you like to store it in another way too?: 5
```

8. To create and update the https bindings in IIS server, choose 1.

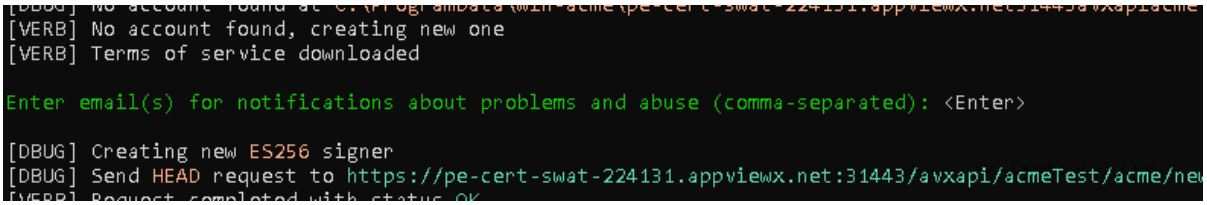
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



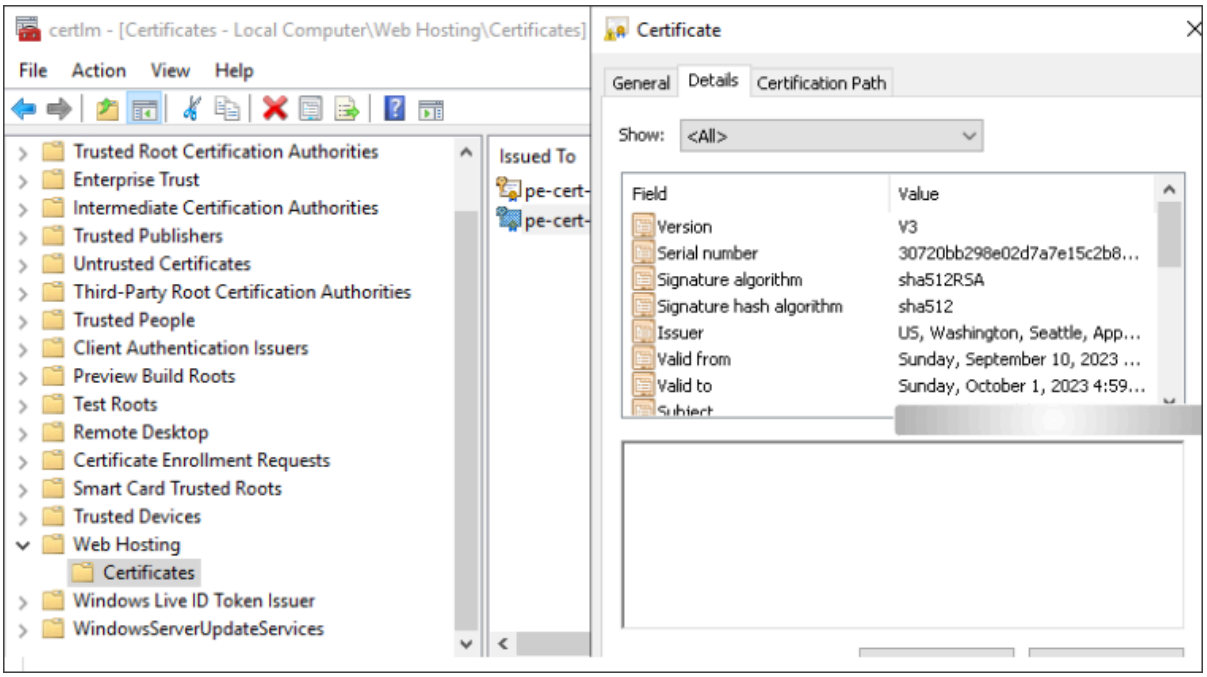
9. Enter 4 to add no other installation steps and continue.



10. Provide an email address or press enter to skip.



11. The certificate will be bound to the chosen IIS server and the certificate will be stored in the Windows certificate store.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Using PowerShell Script

win-acme is initiated as a hidden process using a PowerShell script. When the PowerShell script is run, the terminal opens in the background and remains invisible to the user.

Steps to run the win-acme enrollment process in background:

1. Choose the script as per the requirement and follow these steps:
   - **Run win-acme using manual hostname as input:** The following PowerShell script fetches the certificate for the hostname specified and binds it with the IIS server for the site ID specified.

```
$wacsPath = "<path to the wacs.exe file>"
$arguments = "--validationmode HTTP-01 --source manual --host <host-name> --emailaddress <email id (or) NA> --installation iis --installationsiteid <site id> --verbose --eab-key-identifier <eab-key-identifier> --eab-key <eab-key> --eab-algorithm <eab-algorithm>"
Start-Process -FilePath $wacsPath -ArgumentList $arguments -WindowStyle Hidden
```

> **Note:** The command `--eab-key-identifier -O7R97x8T52ASpwAYZJzJ --eab-key _Pqh5h6yJKThrXiqy6GGsfVIZdgNNw --eab-algorithm HS256` is only applicable when EAB is enabled in the server side.

   - **Run using CSR as input for certificate generation:** The following PowerShell script fetches the certificate using the given CSR file and binds the certificate to the specified site ID.

```
$wacsPath = "<path to the wacs.exe file>"
$arguments = "--validationmode HTTP-01 --source csr --csrfile <Path to the csr file> --pkfile <Path to the key file> --emailaddress <email id (or) NA> --installation iis --installationsiteid <site id>  --verbose"
Start-Process -FilePath $wacsPath -ArgumentList $arguments -WindowStyle Hidden
```

   - **Run using site ID as input for certificate generation**
     - Multiple site IDs can be given in comma separated format in this script (for example, 1,2,3).
     - This PowerShell script fetches the hostnames of the servers mentioned in the <site ID> and creates a single certificate.
     - The hostnames of all the specified IIS servers are present in the SAN DNS of that certificate.
     - All the servers mentioned in the <site ID> are bound with the same certificate.
     - This is not applicable for IP based binding and only works for hostname based bindings.

```
$wacsPath = "<path to the wacs.exe file>"
$arguments = "--validationmode HTTP-01 --source iis --siteid <site id>  --emailaddress <email id (or) NA> --installation iis --verbose"
Start-Process -FilePath $wacsPath -ArgumentList $arguments -WindowStyle Hidden
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The command `--eab-key-identifier -O7zaR976x8T52AGASpwAAAYZJzJ --eab-key _PqhM5h6yJnXKThr7Xiq4y6GGlFsfGVICZdgNNw --eab-algorithm HS256` is only applicable when EAB is enabled in the server side.

Refer to these points to replace placeholder values in the commands:

- `<path to the wacs.exe file>`: The wacs.exe file path (present inside the win-acme installation folder).
- `<host-name>`: The hostname for which the certificate needs to be acquired.
- `<site id>`: This ID can be found in the IIS server manager.
- `<email id (or) NA>`: An email address or NA (should not be empty). This is bound to the win-acme account.
- `<Path to the csr file>`: Path of the CSR file.
- `<Path to the key file>`: Path of the key file associated with the given CSR.

2. Save the required script in .ps1 format (the new ps1 file can be created using Windows PowerShell ISE > File > New).
3. Open PowerShell with admin privileges.
4. Run `.\<shell script file name>`
5. To ensure that the task is being run in the background, open the Windows Task Manager and look for the *wacs* process (This may be found as separate process or under Windows PowerShell process).
6. If the manual approval is enabled in the CA policy settings, this process waits for the certificate to be approved. (The client polls the ACME server for the certificate according to the *RetryCount* and *RetryInterval* values provided in the settings.json file. [Path - C:\AppViewX_ACME_Winacme_Client\winacme\settings.json].
   After receiving the certificate, this process is terminated. The certificate is found in the Windows certificate store (under the Web Hosting/certificates tab).

DNS-based Challenge Validation

DNS-based challenge validation in the ACME protocol involves proving the domain ownership by adding a specific TXT record to the domain's DNS records. When the ACME server issues a certificate for a domain, it provides the ACME client with a unique challenge token. The ACME client then adds this token as a TXT record in the domain's DNS configuration. AppViewX verifies the domain ownership by querying the DNS records for the challenge token. Once the token is found, the validation is considered successful and the certificate is issued.

This method of validation requires access to modify DNS records for the domain typically through the domain registrar or DNS-hosting provider.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Extract the route53 plugin zip file in the win-acme folder.
2. Open a command prompt terminal in the win-acme folder and run the following command:

```
wacs.exe --verbose --validation route53
```

3. Continue with the enrollment process as mentioned in the Section, *Steps for using M: Create Certificates with Full Option* until you reach the step where the challenge method is chosen.
4. Select **Create verification records in AWS route 53** option.

```
1: [http] Save verification files on (network) path
2: [http] Serve verification files from memory
3: [http] Upload verification files via FTP(S)
4: [http] Upload verification files via SSH-FTP
5: [http] Upload verification files via WebDav
6: [dns] Create verification records in AWS Route 53
7: [dns] Create verification records manually (auto-renew not possible)
8: [dns] Create verification records with acme-dns (https://github.com/joohoi/acme-dns)
9: [dns] Create verification records with your own script
10: [tls-alpn] Answer TLS verification request from win-acme
C: Abort

How would you like prove ownership for the domain(s)?: 6
```

5. Enter the Route53 credentials when prompted.
6. Follow the steps as shown:

```
How would you like prove ownership for the domain(s)?: 6

[VERB] No value provided for --route53iamrole

Description:         AWS IAM role for the current EC2 instance to login into
                     Amazon Route 53. Note that you should provide the IAM
                     name instead of the ARN.

IAM role name (leave blank to use access key): <Enter>

[VERB] No value provided for --route53accesskeyid

Description:         Access key ID to login into Amazon Route 53.

Access key ID: [redacted]

[VERB] No value provided for --route53secretaccesskey

Description:         Secret access key to login into Amazon Route 53.

1: Type/paste in console
2: Search in vault

Choose from the menu: 1

Secret access key: ****************************************

Save to vault for future reuse? (y/n*) - no
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

On completion, the enrollment process begins and the certificate is issued upon successful validation of the DNS challenge.

Note: This is a sample to use the DNS route 53 plugin for challenge validation. Users can use the other DNS plugins also for validation. Refer to the following link to use the other DNS plugins: https://www.win-acme.com/reference/plugins/validation/dns/

Default Challenge Validation

This challenge requires you to prove control over the DNS for a domain by adding a specific value to a TXT record within that domain. AppViewX then performs a DNS query to verify the presence of the token in the domain's DNS records.

A sample command to do the challenge validation using the AWS route 53 server is as shown:

```
wacs.exe --target manual --host <domain name> --validation route53 --validationmode dns-01 --route53accesskeyid <route53 key id> --route53secretaccesskey <route53 key>  --eab-key-identifier <EAB key identifier> --eab-key <EAB HMAC key> --eab-algorithm <EAB alogrithm>  --verbose  --emailaddress <mail address>
```

DNS Challenge Validation (using AppViewX DNS plugin with Infoblox DNS Server)

This challenge requires you to show how AppViewX manages DNS for the domain by adding a specific value to a TXT record within that domain. AppViewX then performs a DNS query to verify the token's presence in the domain's DNS records. AppViewX, with the support of Platform Integration Hub, will handles all aspects of creating, searching, and deleting TXT records in the DNS server.

A sample command to do the AppViewX DNS Challenge Validation option is as shown:

```
wacs.exe --target manual --validation appviewx --host <domain name> --vendor infoblox --vendoraccountname <Infoblox server name configured in appviewx> --validationmode dns-01 --eab-key-identifier <Key identifier> --eab-key <HMAC key> --eab-algorithm <EAB Algorithm> --verbose --emailaddress <email address>
```

Enterprise Secure Challenge Validation

This challenge requires you to show how AppViewX manages DNS for a domain by querying to verify the presence of the client's IP address in the domain's DNS A record. This verification does not require DNS server credentials as it only involves accessing the DNS A record for the specific domain.

A sample command to do the AppViewX Enterprise Secure Challenge Validation option is as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
wacs.exe --target manual --validation appviewx --host <domain name> --validationmode dns-01 --eab-key-identifier <key identifier> --eab-key <HMAC key>
 --eab-algorithm <EAB Algorithm> --verbose  --emailaddress <email address>
```

DNS Challenge Validation using Azure Plugin

Enrolling Certificates for Public DNS

```
wacs.exe --target manual \
--host <FQDN_NAME_FOR_CERTIFICATE>\
--validation azure \
--azuretenantid xxx-xxx-xxx \
--azureclientid xxxxxxxxx \
--azuresecret xxxxxxxxx \
--azuresubscriptionid xxx-xxx-xxx \
--azureresourcegroupname xxx \
--eab-key-identifier <key_identifier> \
--eab-key <hmac_value> \
--eab-algorithm <eab_algorithm>
--emailaddress <eab_email_address>
```

Enrolling Certificates for Private DNS

```
wacs.exe --target manual \
--host <FQDN_NAME_FOR_CERTIFICATE>\
--validation azure \
--azuretenantid xxx-xxx-xxx \
--azureclientid xxxxxxxxx \
--azuresecret xxxxxxxxx \
--azuresubscriptionid xxx-xxx-xxx \
--azureresourcegroupname xxx \
--eab-key-identifier <key_identifier> \
--eab-key <hmac_value> \
--eab-algorithm <eab_algorithm>
--emailaddress <eab_email_address>
--azurezonetype private
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Renewing Certificates

Scheduling Tasks

A scheduled task renews certificates when necessary, based on the specified threshold in the settings.json file. The program checks certificates daily to see if they are close to expiration. The settings.json file also controls how long cached certificates can be used for renewals.

The following are configuration settings in the settings.json file located within the win-acme directory:

Adjusting settings in the Cache field

- Adjust the value of **ReuseDays** to **0**:

  When renewing or creating a certificate with the same domain names as before, **ReuseDays** decides how long the program will use a cached version. Setting **ReuseDays** to **0** stops using cached files for renewals.

  The default value for **ReuseDays** is set to **1**.

Adjusting settings in the ScheduledTask field

1. Set **RenewalMinimumValidDays** to determine the minimum number of days a certificate should remain valid. If a certificate has fewer days left than this threshold, automatic renewal will be triggered.

   The default value for **RenewalMinimumValidDays** is set to **null**, which is interpreted as 7 days.

   For example: If you set the parameter to 10, certificates with less than 10 days validity will be renewed automatically using the task scheduler. Certificates with 10 days or more remaining will not be renewed.
2. Adjust the **StartBoundary** to specify the start time for the scheduled task.

   The default value for **StartBoundary** is set to **09:00:00**, which is interpreted as 9:00 am (local time).
3. [Optional]: Set **RandomDelay** to **00:00:00** (0 hour), which is the time to wait before starting the scheduled task to spread the load on the servers and thus prevent users from getting TooManyRequests errors.

   The default value for **RandomDelay** is set to **04:00:00**, which is interpreted as 4 hours.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Health Checks

The health of the scheduled task is checked each time the program is run manually. It can also be (re)created from **More options > (Re)create scheduled tasks**.

Monitoring

The renewal process can be monitored from the Windows Event Viewer and log files written to `%programdata%\win-acme\$baseuri$\Log`.

Scheduling Tasks for Auto-Renewal

win-acme schedules task using the configurations from settings.json file. For more information, see Renewing Certificates.

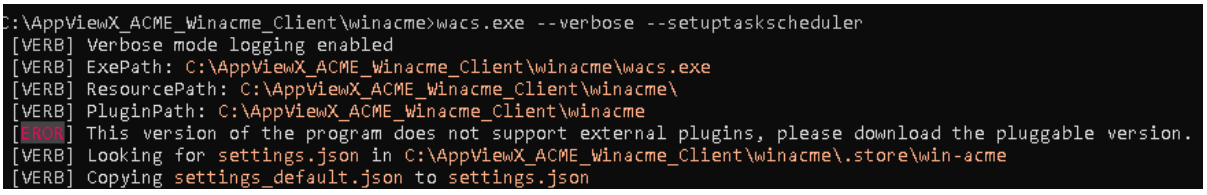
> **Attention:** Ensure that you have removed the .store directory within the win-acme folder. Neglecting this step might result in the creation of a scheduled task using parameters from the previous settings.json configuration disregarding the recent adjustments.

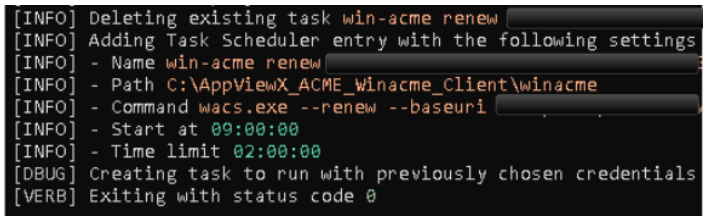
It is possible to create a renewal task for win-acme in Windows using either a command or an interactive terminal session.

Using Command

1. Open command prompt with admin privilege and run:

```
wacs.exe --verbose --setuptaskscheduler
```





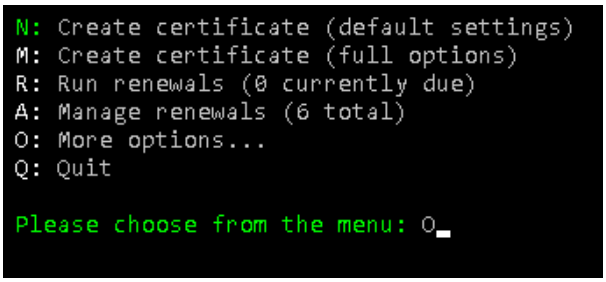
2. Ensure that the **Start at** time in the end of the log matches with the **StartBoundary** time specified in the settings.json file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

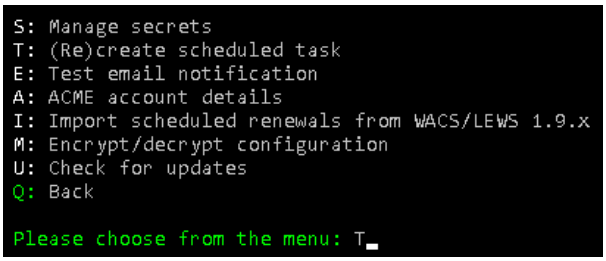
Using Interactive Terminal

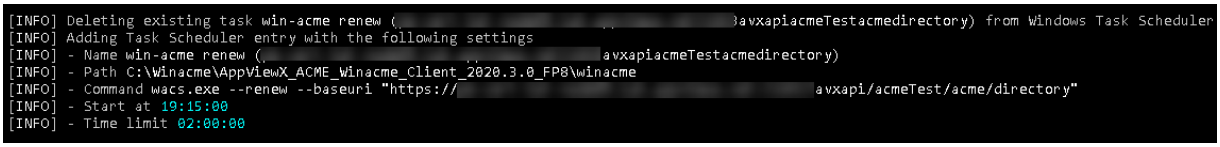
1. Run the following command and choose option O to go into More Options:

```
wacs.exe --verbose
```



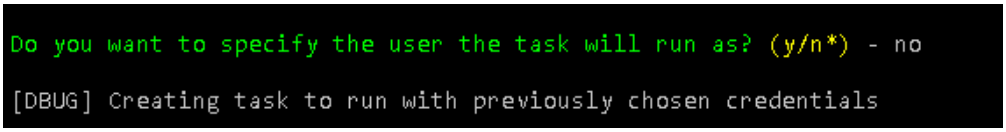
2. Choose option T.





Ensure that the **Start at** time aligns with the **StartBoundary** time specified in the settings.json file.

3. Type n.



This sets up a scheduled task in the Windows Task Scheduler for the renewal of win-acme using the parameters specified in the settings.json file.

> **Note:** You can cross verify by refreshing the Task Scheduler Library to find the **win-acme renew** task. Check if the **Next Run Time** of this task matches the defined **StartBoundary** time.

Points to be noted:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Whenever the scheduled **win-acme renew** task is triggered, the newly generated certificates from the renewal process will take the place of the older certificates in the **Certificates - LocalComputer \Web Hosting\Certificates** section present within the **Manage computer certificates** console.
- Certificates that have a remaining validity period that is equal to or greater than the specified **RenewalMinimumValidDays** will not be subjected to renewal and will remain unaltered in the certificates console.
- After scheduling a win-acme renewal task using the specified settings.json, the task will continue to operate with those configurations until a new win-acme renewal task is generated with altered settings.
- Later on, if you want to (re)create a scheduled task for winacme renewal, simply go through the steps **a** and **b** as described earlier. This will overwrite any existing winacme renewal task in the task scheduler, if there is one.
- Other properties of the scheduled task like **RenewalDays**, **ExecutionTimeLimit** can also be changed in a similar manner. Some of these parameters can be changed from the Task Scheduler itself, as long as the name is not modified.

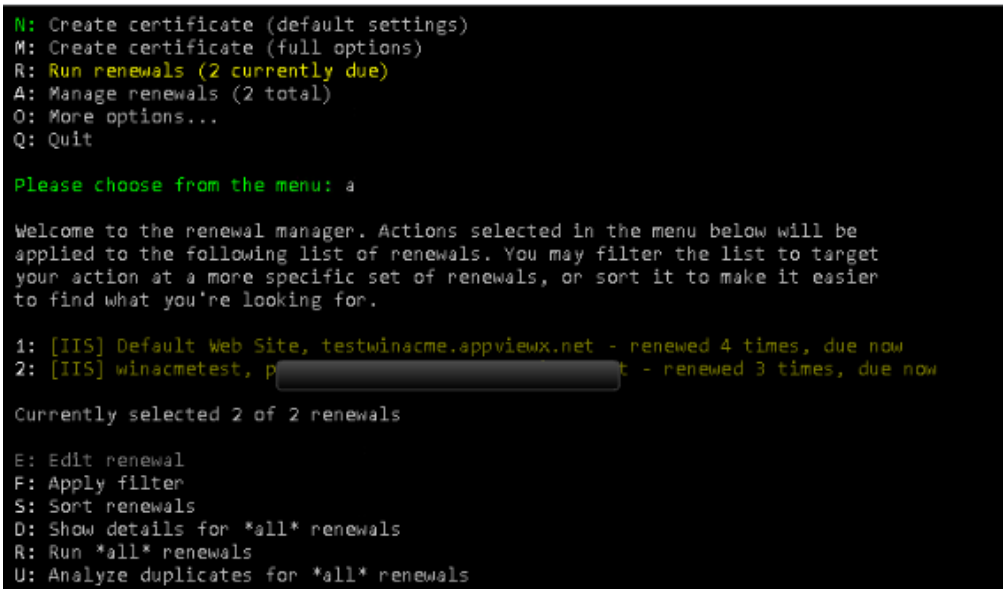
Revoking Certificates

Revoking a certificate must be done only when the private key is believed to have been compromised, and not when simply replacing or canceling the private key. Revocation can be done from **Manage renewals > Revoke certificate**.

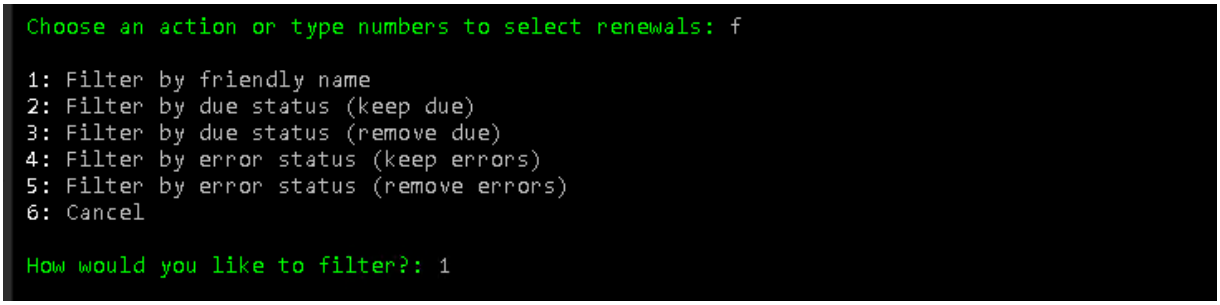
To revoke a certificate in win-acme:

1. Run `wacs.exe`.
2. Enter A to list the certificates. These names can be used to revoke a particular certificate.

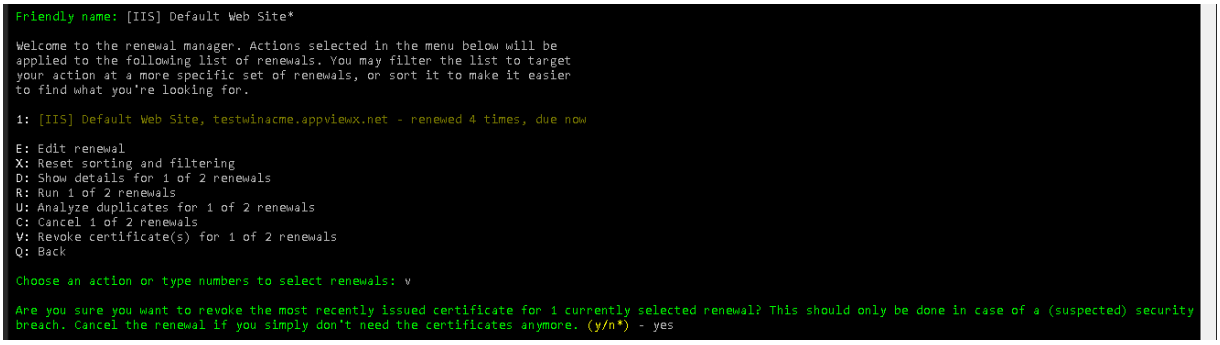
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



3. Enter V to revoke all certificates. If one particular certificate is to be revoked, then use F option to apply filter.



4. If F is chosen, this menu will be prompted. Enter 1 to filter by friendly name.



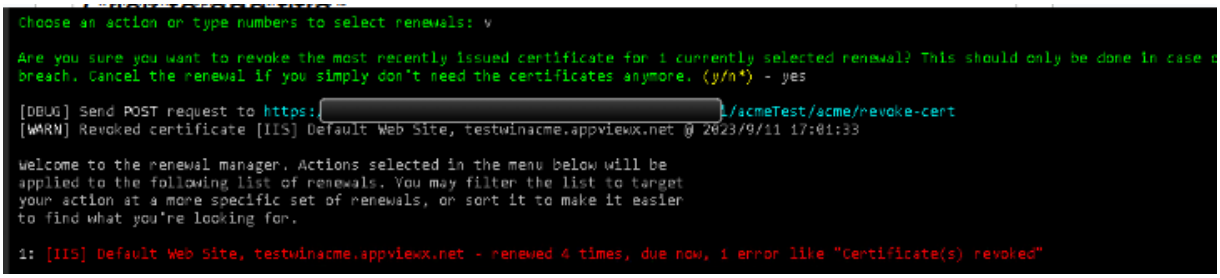
5. Enter the friendly name as shown (Friendly names are displayed in Step 1):

Example 1	If the name displayed in the menu is [IIS] winacme-test, pe-cert-swat-142107.appviewx.net, then enter the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

	following in the friendly name filter → `[IIS] winacme-test*`
Example 2	If the name displayed in the menu is `[IIS] Default Web Site, testwinacme.appviewx.net`, then enter the following in the friendly name filter - `[IIS] Default Web Site*`

6. Verify if the intended certificate is filtered.
7. Enter V to revoke the selected certificate and type yes for the revoke prompt as shown:



Issuing Certificates using Tomcat Server

To issue a certificate with win-acme using the Tomcat server for challenge validation, run:

```
wacs.exe --verbose --target manual --validation filesystem --host <server-domain-name> --webroot "<complete-path-of-tomcat-webapps-folder>"
```

Sample command:

```
wacs.exe --verbose --target manual --validation filesystem --host test.appviewx.net --webroot "C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps"
```

Note: --webroot "<complete-path-of-tomcat-webapps-folder>": This should point to the location where Tomcat serves its web applications. The certificate will not bind to the server with this command.

Issuing and Binding Certificates using Tomcat Server

1. While win-acme does not include a native plugin for binding certificates to the Tomcat server, the following command can be used to leverage the installation script option in win-acme:

```
.\wacs.exe --verbose --target manual --validation filesystem --host <server-domain-name> --webroot "<complete-path-of-webapps-folder>" --store pfxfile --pfxfilepath "<pfx-file-folder>" --pfxpassword <pfx-password> --accepttos --pfxfilename <pfx-file-name> --installation script --script "<script.ps1 file>"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

where:

- <server-domain-name>: The actual domain name for which the certificate is requested (e.g., example.com).
- <complete-path-of-webapps-folder>: This should point to the location where Tomcat serves its web applications.
- <pfx-file-folder>: The directory where the PFX file will be saved (e.g., C:\path\to\output\folder).
- <pfx-password>: The password used to encrypt the PFX file, securing the private key.
- <pfx-file-name>: The desired name for the PFX file to be created (e.g., mycert).
- <script.ps1 file>: The full path to the PowerShell script that will run after certificate issuance (e.g., C:\path\to\your\script.ps1).

Sample command:

```
.\wacs.exe --verbose --target manual --validation filesystem --host test.appviewx.net --webroot "C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps" --store pfxfile --pfxfilepath "C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf" --pfxpassword Test@1234 --accepttos --pfxfilename cert2024.appviewx.com --installation script --script "C:\Users\admin\Desktop\restart_tomcat_9.ps1"
```

2. Sample PowerShell Script to restart the Tomcat service:

```
Restart-Service -Name 'Tomcat9'
```

The following operations are performed when this command is run :

1. Perform challenge validation using Tomcat on port 80 to obtain the certificate.
2. Export the PFX file with the required password and file path.

> **Note:** This file is referenced in Tomcat's server.xml. This allows win-acme to automatically replace the certificate as needed.

3. PowerShell (.ps1) script that restarts the Tomcat server is run after the certificate is issued, ensuring the new certificate is bound to the Tomcat instance.

Support for other .NET Versions

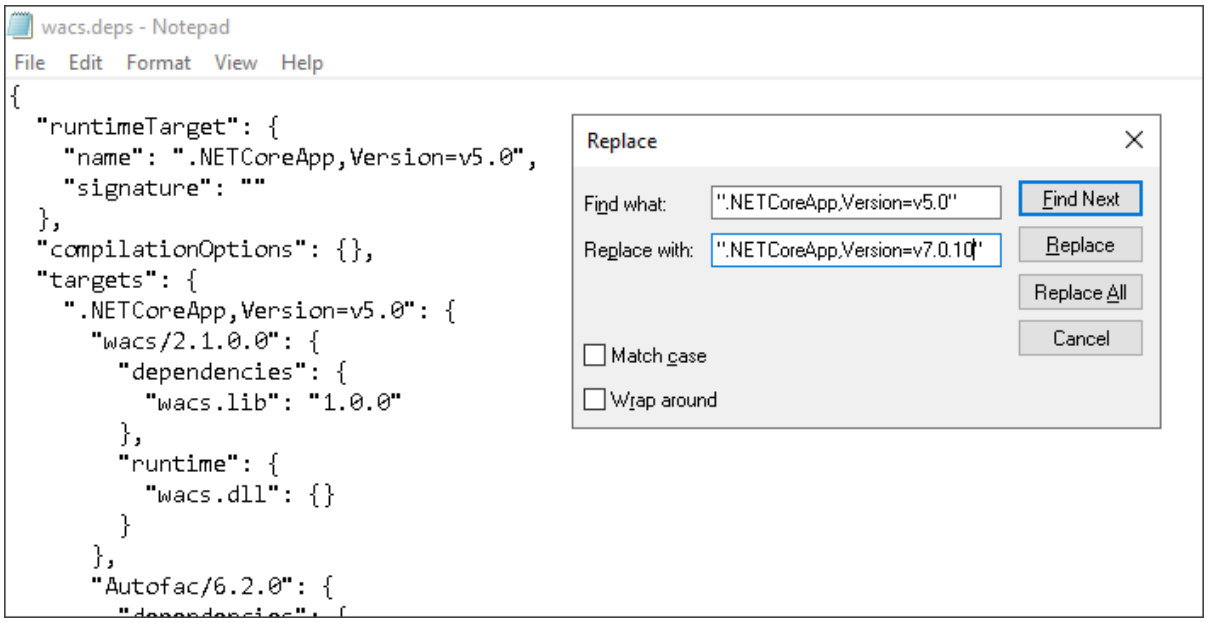
win-acme supports .NET v5. For newer .NET versions, the configurations in `wacs.dep` and `wacs.runtimeconfig` need to be changed. These files are found in the win-acme folder.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Changes in the wacs.dep file

- Use CTRL+H to open the *find and replace* menu to replace `.NETCoreApp,Version=v5.0` with `".NETCoreApp,Version=v<version of .NET in the pc>"`
- Use the complete version number when replacing, such as 7.0.10

  For example: `".NETCoreApp,Version=v5.0"` is replaced with `".NETCoreApp,Version=v7.0.10"`



- Similarly replace (replace all) `"Microsoft.NETCore.Platforms": "5.0.0"` with `"Microsoft.NETCore.Platforms": "<version of .NET in the pc>"`.

Changes in the wacs.runtimeconfig file

- Replace (use replace all) `"tfm": "net5.0"` with `"tfm": "net<version of .NET in the pc>"`
- Replace `"version": "5.0.0"` with `"version": "<version of .NET in the pc>"`.

Best Practices

- **Prefer Stronger Key Sizes:** Use higher key sizes where applicable—consider using RSA 2048 or above for increased cryptographic strength.
- **Distribute Renewal Schedules:** Ensure that certificate renewal cron jobs or schedulers are spread out in time to avoid concentrated load on the ACME server and ensure smooth, uninterrupted renewals.
- **Use External Account Binding (EAB):** Use EAB as an added layer of authentication for enhanced security.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Secure your API credentials:** Store DNS provider API keys securely (e.g., environment variables, encrypted files).
- **Challenge Methods:** Prefer **DNS-01 challenge** when possible using supported DNS APIs. For **HTTP-01**, ensure port 80 is reachable and forwarded correctly if behind a NAT or firewall.
- **Scripting & Hooks:** Use pre- and post-renewal scripts to restart IIS or services and to copy certificates to remote locations or appliances.
- **Storage:** Use --store and --installation parameters wisely to define multiple cert storage and bindings (IIS, file, registry, etc.).
- **Logging:** Enable **verbose logging** and monitor the renewal logs at C:\ProgramData\win-acme\logs.
- **Custom Package Verification:** Make sure the AppViewX DNS plugin is available in Winacme package if the user is using the AppViewX DNS Challenge or the Enterprise Secure DNS Challenge option.

Troubleshooting

Accessing ACME Logs

1. Access the terminal window.
2. Go to <Installed_Path>/logs directory and find the name format with <avxgw-HTTPS-<yyyy-mm-dd>.log>. For example, <avxgw-HTTPS-2021-03-17.log>
   - If the file size exceeds 100MB, it will be rolled over and the latest logs will be available in the latest file named with an incrementing counter starting from 1 such as avxgw-HTTPS-<yyyy-mm-dd>.<incrementing_counter>.log, for example, <avxgw-HTTPS- 2021-03-17.1.log>.
   - ACME plugin logs:

     </home/appviewx/appviewx/logs/avx-vendor-cert-acme-agent-<pod_name>.log>

Common Issues

- You may need to install Microsoft Visual C++ 2015 Redistributable Update 3
- If you run into an error about api-ms-win-crt-runtime-l1-1-0.dll, refer to KB2999226.
- If you run into an error about hostfxr.dll, refer to KB2533623.
- If you run into an error such as Failure processing application bundle, perhaps this thread might provide a solution.
- If the program does not seem to start but you see an error such as Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy:App.AppXc99k5qnnsvxj5szemm7fp3g7y08we5vm.mca in the Event Viewer, this thread might provide a solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Scenarios

To troubleshoot the renewal process, renewals can be triggered manually from the menu. When listing the details for renewal, the program displays any errors that have been recorded during the previous runs.

#	Error Message	Description	Troubleshooting
1	Unable to connect to ACME server System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.Http.WinHttpException (80072EE7, 12007): Error 12007 calling WINHTTP_CALLBACK_STATUS_REQUEST_ERROR, 'The server name or address could not be resolved'.	The default base uri name is not configured in the settings.json / the configured URL or the port is wrong.	Configure the correct URL in the default base uri section in settings.json file.
2	Initial connection failed	1. Configured Agent settings URL might be incorrect. 2. AppViewX Server / CC might not have a valid certificate. 3. Certificate bound to AppViewX server/CC might not be trusted by the Windows machine.	1. Check the value DefaultBaseUri in the settings.json, it should be the same as ACME URL in AppViewX GUI. Always use the hostname instead of IP while configuring the ACME end point in AppViewX GUI. 2. Bind a valid certificate to the gateway. 3. The certificate that is bound to the AppViewX server / Cloud Connector should be trusted by the windows client machine, that is, the root

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
			and intermediate certificates associated with the bound certificate must be added to the Windows root and intermediate trust stores.
3	Failed to create order: Unable to fetch acme server url. - Agent Settings name given is invalid	The Agent name provided in the URL is incorrect / Agent setting is not configured in the ACME server side configuration.	Check the status of the ACME end point in AppViewX GUI. It should be in Valid status. If it is in failed status, check the reason for the same and fix it. 1. Agent settings failed in ACME services step, then the ACME pod is not enabled in AppViewX. Enable the same 2. Agent settings validation failed in CA Settings Step, then check in the CA settings page check the test connection status of the ACME endpoint configured CA, it might be

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
			in New or Failed status. 3. Make sure the test connection is successful for the CA and go to ACME page and check the status of ACME end point and make it as valid.
4	Authorization Invalid (Challenge validation failed)	**HTTP** 1. The common name used is not resolved to the client machine. 2. Client machine and port 80 might not be reachable from AppViewX. **DNS** win-acme might not be able to access the DNS server to add the txt record. **HTTP**	**HTTP** 1. Check if the common name used in the certificate is resolving to the client machine, if not make an appropriate entry in the local DNS server. 2. Check the firewall rules and make sure that client machine is reachable from AppViewX / CC and port 80 is open for inbound traffic. **DNS** Check if the DNS server credentials

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
			provided in win-acme is a valid one. Check if the Windows machine has internet access to access the DNS server to add the TXT records. Check if AppViewX or CC has internet access to read the TXT records.
5	No sites with host bindings have been configured in IIS	IIS server in windows client is: • Not enabled • Not in running state • Bindings does not have a valid hostname	Check the following in the IIS server configuration: • IIS server is enabled • Site should be configured and be in running state • Binding should have a valid value in the Hostname field. (The hostname should have an entry in local DNS server and resolving to same Windows machine IP.)
6	Requested account not available.	Account that client is trying to use for enrollment is not available on the server.	Go to C:\ProgramData\win-acme\ folder and then go inside the agent folder

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
			and delete the Registration_v2 file
7	Unable to perform ACME order finalize operation - Either CSR Parameters,CA details or certificate algorithm values are not compliant with the policy name - <Policy Name>	CSR parameters from the client are not matching with parameters configured in AppViewX policy.	Check if the policy is set as strict. • Change the policy type to Suggestive. OR • Configure the CSR parameters as per the policy requirements (Cert policy in AppViewX)
8	Unexpected order status processing (Exception): Unable to complete order	Certificate issuance is still in progress or failed.	Navigate to the holistic view of the certificate in AppViewX and check for the work order status: • **In progress:** CA is taking time to issue the certificate. Increase the retry count and frequency. • **Failed:** Click the work order and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
			check the reason for failure and remediate it.
9	Self DNS Challenge token validation/IP Validation option is selected but EAB details/Allowed domains are not configured for the agent settings.	When AppViewX **DNS Challenge** or **Enterprise Secure Challenge Validations** is selected but **Allowed Domains** or EAB details are not provided from the ACME client, you get this error.	1. Provide valid domains under the **Allowed Domains** field. 2. Enable either **Static EAB** or **Dynamic EAB credentials**.
10	DNS Challenge validation failed. IP Options are not selected for agent settings. Allowed options are STRICT, ANY, NONE.	If Enterprise Secure Challenge type other than **Secure, Any, Ignore** is selected in the ACME Settings.	Select any one of the following under Enterprise Secure Challenge options: **Secure, Any, Ignore.**
11	DNS Challenge validation failed. ACME DNS challenge verification via DNS A record failed. For STRICT Option IP didn't Match.	If the **Secure** option is selected under **Enterprise Secure Challenge** type and the ACME client’s IP address does not match with the available DNS	Make sure that the DNS A record of the requesting domain contains the same IP address as the ACME client's IP address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
		A record for the particular domain.	
12	DNS Challenge validation failed. ACME DNS challenge verification via DNS A record failed. For STRICT Option there are more IP address entries in DNS A Record.	If the **Secure** option is selected under **Enterprise Secure Challenge** type and the DNS A record for the requesting domain is fetched with more than one IP address.	Make sure that the DNS A record of the requesting domain contains only one IP address, which is the same as the ACME client's IP address.
13	DNS Challenge validation failed. No DNS A records are found to validate ANY type.	If the **ANY** option is selected under **Enterprise Secure Challenge** type and the DNS A records for the requesting domain are fetched in which none of the IP address matches with the ACME client’s IP address.	Make sure that the DNSA records of the requesting domain contains any one IP address, which is the same as the ACME client’s IP address.
14	DNS Challenge validation failed. DNS A record for the domain <domain name> is not available.	When AppViewX is not able to obtain the DNS A records for the requesting domain.	• Check if the DNS Server is reachable from AppViewX to resolve and obtain the DNS A records

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
			of the requesting domain. • Check if the provided DNS server hostname is proper to resolve and obtain the DNS A records.
15	DNS Challenge validation failed. Error while executing Create/Delete record operation.	1. When AppViewX is not able to reach the DNS server for creating DNS TXT for the requesting domain. 2. When there are errors while performing creation or deletion of DNS TXT records in the DNS server.	1. Check if the DNS server is reachable from AppViewX. 2. Check AppViewX logs for detailed errors regarding creation and deletion of errors.
16	[ERR] (WinHttpException): Error 12002 calling WINHTTP_CALLBACK_STATUS_REQUEST_ERROR, 'The operation timed out'.	This issue occurs during the challenge validation process. When validation fails, it is often due to the firewall	Configure the firewall to allow AppViewX server/CC to access port 80 of the win-acme machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
		or Microsoft Defender blocking the AppViewX server or CC from accessing port 80 on the Windows machine.	

Keywords Used in win-acme Commands

Keyword	Expected Input	Comments
-host	<Domain_Name> (Type: String) **domain1.com** (or) **domain1.com, domain2.com, domain3.com**	Comma-separated list of domains to obtain a certificate for.
-baseuri	<Acme Server Endpoint URL fetched from AppViewX GUI> (Type: String)	ACME Directory Resource URI.
-source	csr/iis/manual	Source using which the CSR is generated

Configuring AppViewX Certbot Client

What is Certbot?

Certbot is a popular open-source tool for automating the process of obtaining and managing SSL/TLS certificates. It acts as an ACME (Automated Certificate Management Environment) client, which is a protocol used by certificate authorities (CAs) to issue certificates. The Certbot agent provides a command-line interface (CLI) and automation capabilities to simplify the certificate management process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

It handles the entire certificate lifecycle, including certificate generation, renewal, and installation. Certbot automates the process of obtaining certificates from Let's Encrypt, a free and open certificate authority, which is the default option but can be configured to work with other CAs as well. Certbot is a powerful and user-friendly tool that simplifies the deployment and management of SSL/TLS certificates, promoting the widespread adoption of secure HTTPS communication on the web.

Note:

The inherent challenges of using native Certbot include the issuance of certificates without common names, the absence of support for custom attributes, the need for manual installation of Certbot dependencies and virtual environments, and the lack of a user-friendly terminal experience.

Our solution addresses these limitations comprehensively by providing certificates with common names. It supports custom attributes, automates dependency installation and virtual environment setup required for Certbot to run, and offers a user-friendly terminal. These enhancements improve functionality and user experience significantly.

Advantages of AppViewX Certbot

- Single-click installation and interactive digital certificate CLM operations.
- Support for working with Let’s Encrypt CA through AppViewX (where AppViewX acts like an ACME Proxy to Let’s Encrypt CA).
- Custom attribute and certificate attribute support in Certbot command for enrollment and renewal.
- Addition of CA Certificate in native trust store for the ACME client to work with any CA issued SSL Server certificate.

Getting Started

Prerequisites

- The AppViewX server/cloud connector must be bound with a valid certificate. See Section, *Binding Custom Certificate to Gateway in Cloud Connector*.
- Ensure you have root user permissions.
- A proper DNS entry for the Linux server where Certbot is installed.
- Certificate attributes must be configured to capture custom attributes in the AppViewX GUI (if required).
- A valid ACME endpoint must be configured on the AppViewX GUI.
- To enable client connections, it is essential to have ports 31443 open for on-premises deployment and port 30020 (in cloud connector) open for SaaS deployment in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- If the domain validation is done using **HTTP challenge**, it is essential to have port 80 accessible on your Linux machine to allow AppViewX to establish a connection.
- If the domain validation is done using **DNS challenge**, then the DNS server must be up and running and the DNS credentials must be configured in the Certbot client.
- Internet connectivity is required to successfully install the Certbot client.

System Requirements

- **Environment Details:** Linux
- **Operating System:**
  - Ubuntu 20.4
  - CentOS 7
  - Red Hat 8.6
  - Debian 10
  - Devuan 3
  - OpenSUSE Tumbleweed

- **Python 3.8** (Ubuntu 20.4, CentOS 7, Red Hat 8.6)
- **Python 3** (Debian 10, Devuan 3, OpenSUSE Tumbleweed)
- **OpenSSL**
- **Virtual environment (venv) and required dependencies** for Certbot
- **jq package** is a prerequisite (must) to access Interactive digital certificate CLM operations.
- **REQUESTS_CA_BUNDLE environment variable** (custom CA bundle path in the root user's .bashrc file) which is required to enable SSL verification. The root certificates trusted by Certbot can be overridden by setting the REQUESTS_CA_BUNDLE environment variable.

If any of the above packages are not installed or configured in your system, AppViewX will do it for you without any human intervention.

Installing Certbot

Certbot comes in two versions: open-source and the one provided by AppViewX. When using the open-source Certbot via AppViewX, the Common Name field will not be filled, and features specific to AppViewX such as custom/cert attributes, customizable EAB algorithms, and CSR options, will be unavailable.

If you are using the open-source Certbot, proceed directly to the certificate enrollment section. Keep in mind that a virtual environment may not be required for enrollment, depending on the version of the open-source Certbot installed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Download the Certbot client from the AppViewX release portal.
2. Open your terminal and go to the directory where you downloaded the Certbot zip file.
3. Unzip the file and open the unzipped folder.
4. To proceed with further installation steps, you must have root privileges. Log on as sudo user using the command:

```
sudo -i
```

Installing Certbot via Automated Installation Files

For automated installation, AppViewX provides a simple installation script [install.sh] that streamlines the setup process, including the creation of a virtual environment and automatic downloading of all required dependencies. To install using the install.sh script, follow these steps:

1. Log on as root user using:

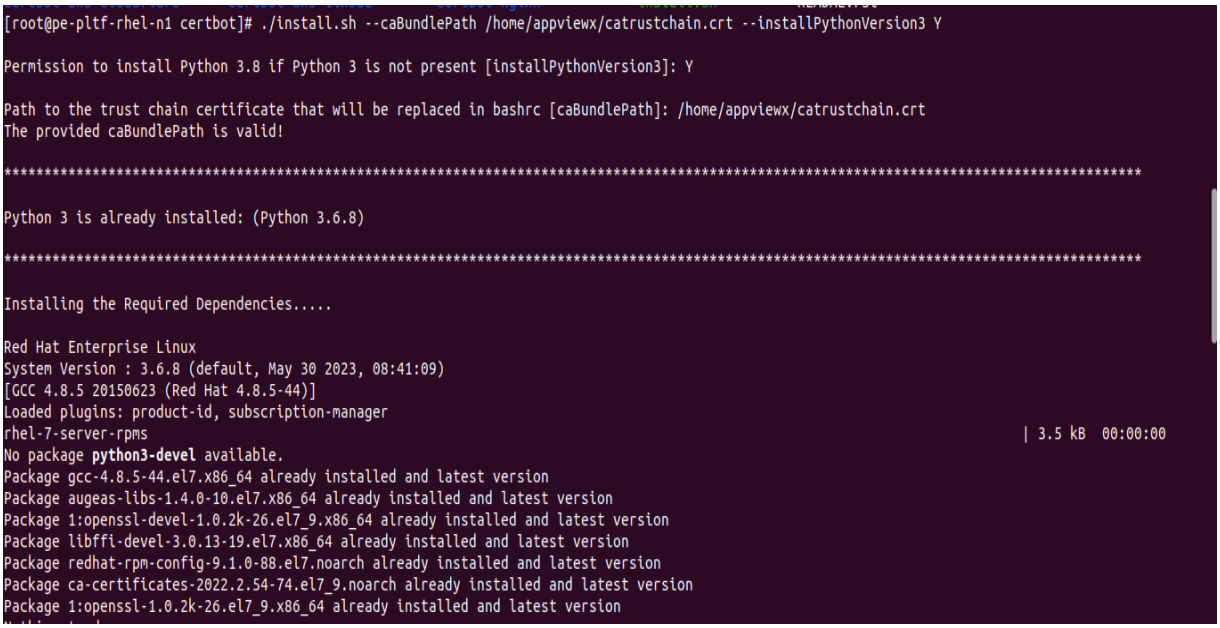
```
sudo -i
```

2. To install dependencies and set up the virtual environment, run:

```
./install.sh
```

You may also pass additional parameters with the install.sh as in the command:

```
./install.sh --caBundlePath /home/appviewx/caCertificate.crt --installPythonVersion3 Y
```



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameter Description

Parameters	Type/ Values	Mandatory	Description
--caBundlePath	Path of the caBundle certificate	No	To strictly enforce SSL verification during the enrollment or renewal of certificates through Certbot, you must provide a custom CA BUNDLE path, indicating the path to your designated trust store file location with the **caBundlePath** parameter. The provided path is used to set the REQUESTS_CA_BUNDLE environment variable in the user's .bashrc file. Alternatively, if you opt to bypass SSL verification during certificate enrollment or renewal via Certbot. Do not provide the **caBundlePath**. In this scenario, the installation process will proceed without having to provide a CA BUNDLE path. However, you will still have the option to activate SSL verification by manually configuring a custom bundle path at a later time. See Section, *Prerequisites*.
--installPythonVersion3	Y (or) N	No (default value : 'N')	The install.sh script examines the Python version present on the client system. If the detected version is below 3, the installation script attempts to install Python 3.8 only if the installPythonVersion3 parameter is configured to Y. If the installPythonVersion3 parameter is set to N, the installation

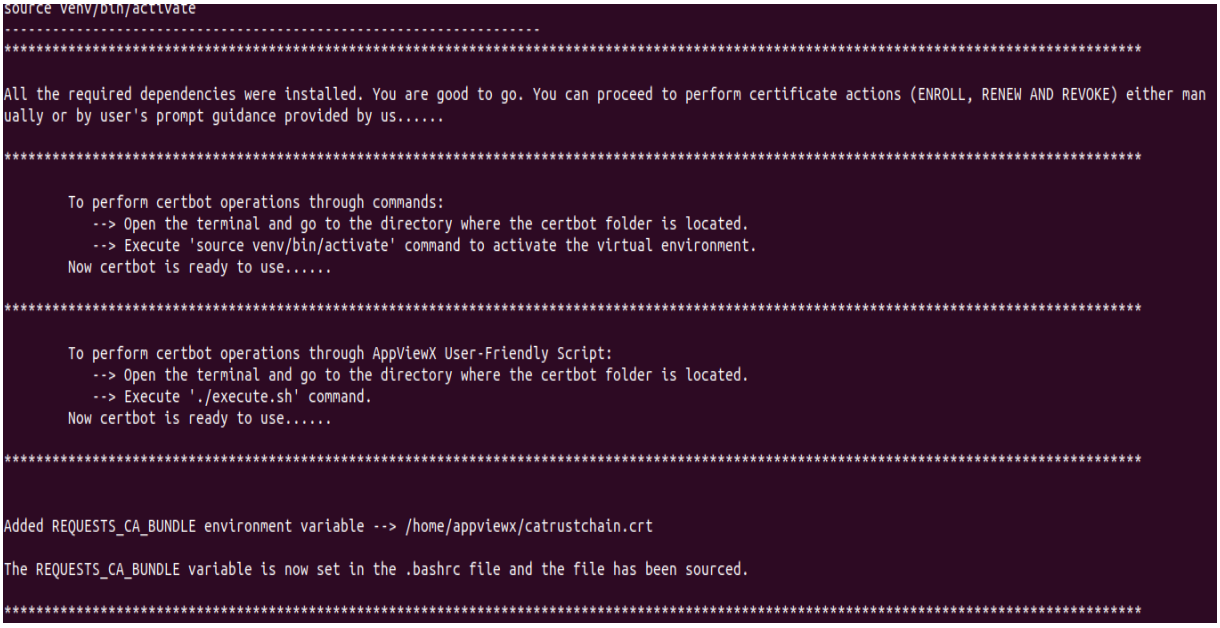
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters	Type/ Values	Mandatory	Description
			process is terminated if Python 3 or a higher version is not found on the client system.

During the installation process:

- The install.sh script verifies the presence of the necessary Python version compatible with the operating system.
- In the event that the required version is absent and the installPythonVersion3 parameter is passed as Y, the script proceeds to install python 3.8.
- The script installs the mandatory Certbot dependencies and establishes the essential virtual environment.

Once the installation is complete, you will see the following details:



Installing Certbot via Commands

To install and to create a Certbot virtual environment manually, follow these steps:

1. Switch to root user using the `sudo -i` command.
2. Install all the required dependencies using:

```
apt install python3-dev gcc libaugeas0 libssl-dev libffi-dev ca-certificates openssl
```

-OR-

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
yum install python3-devel gcc augeas-libs openssl-devel libffi-devel redhat-rpm-config ca-certificates openssl
```

3. Open the Certbot folder using:

```
cd certbot_client/certbot
```

4. Setup the virtual environment running:

```
python3 tools/venv.py
```

A virtual environment is activated within the Certbot folder. You can enroll a certificate, re-enroll, or revoke using the commands mentioned in the Section, Enrolling Certificate.

Installing Bluecat Micetro Plug-In

1. Go to the certbot home directory. Copy the certbot-dns-bluecat-micetro.zip into the certbot home directory.
2. Extract the certbot-dns-bluecat-micetro.zip and ensure that the certbot-dns-bluecat-micetro folder is available in the certbot home directory.
3. Run the following command if virtual environment is configured:

```
source venv/bin/activate
```

4. Run the following command to install Bluecat Plugin:

```
pip install -e <path_to_bluecat_plugin>
```

5. Create a Bluecat credential file with the following values, in the format below:
   - dns_bluecat_micetro_hostname="<bluecat_hostname>"
   - dns_bluecat_micetro_username="<username>"
   - dns_bluecat_micetro_password="<password>"
6. To issue certificate run the following command: (sample command below)

```
certbot certonly -d <FQDN> --preferred-challenges dns --authenticator dns-bluecat-micetro --dns-bluecat-micetro-credentials <bluecat_credentials_file_path>
 --server <ACME_SERVER> --no-verify-ssl
```

Adding Custom CA Certificates to Trust Store

In Certbot, the **--no-verify-ssl** option disables the SSL certificate verification when making HTTPS requests to the ACME server.

If SSL verification is not required, skip the following steps and proceed with enrollment using **--no-verify-ssl.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If SSL verification is required, bind the AppViewX server/CC in both on-prem and SaaS environments with a valid server certificate. Ensure that the issuing CA of the server certificate is trusted by the client machine to successfully complete the SSL verification by following these steps:

Note: Ignore this section if the issuer CA certificates are already trusted by the end machines, or if **--no-verify-ssl** is used, or if the trust has been added via the install.sh script in the previous step.

1. To obtain the certificate chain:
   a. If the server certificate is created in AppViewX, download the chain certificates from the AppViewX inventory; else, download the certificate chain files (.pem or .crt) for the Certificate Authority (CA). This chain must include the root certificate as well as any intermediate certificates of the server.
   b. If there are individual certificates for root CA and intermediate CAs, combine these certificate filesinto a single file. This can be done either through a text editor or by using the command:

      ```
      cat intermediateca.crt rootca.crt > acmetrustchain.crt
      ```

      Here, the intermediate *ca.crt* and *rootca.crt* are sample root certificate files, so change them accordingly. *acmetrustchain.crt* is the final concatenated trust chain certificate.

2. To address situations where Certbot does not trust the SSL certificate employed by the ACME server, add the issuer CA certificates to the appropriate Linux trust store:
   a. Determine the appropriate trust store on your Linux system. Common locations for trust stores are /etc/ ssl/certs/ca-certificates.crt and /etc/ssl/certs/ca-bundle.crt.
   b. Log on as sudo user:`sudo -i`
   c. Go to the directory where the acmetrustchain.crt file is located.
   d. Copy the contents of the certificate chain files and append them to the end of the trust store file using the command: cat acmetrustchain.crt >> /etc/ssl/certs/ca-certificates.crt

      Note to change the trust store part accordingly.

Accessing Certbot

Certbot can be accessed either by:

- Certbot command line
- AppViewX Certbot user-friendly script

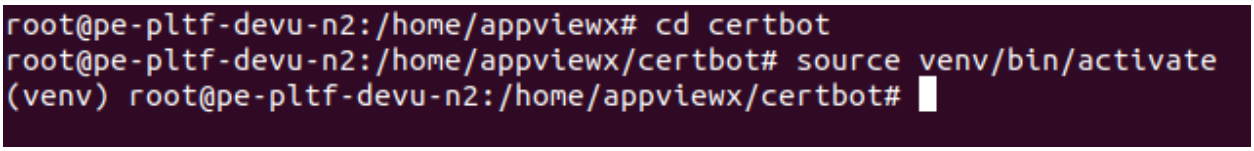
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Method 1: Using Certbot Command Line

Activating Developer Environment

To activate the developer environment, run:

```
source venv/bin/activate
```



Enrolling Certificate

1. **Using HTTP challenge in Standalone Mode**

   HTTP-01 challenge: This is the most common challenge type. The ACME server issues a token to the ACME client, and the ACME client puts a file on the web server at **http://<YOUR_DOMAIN>/.well-known/acme-challenge/<TOKEN>**. Once the token is published on the web server (Linux server), AppViewX sends an HTTP request to fetch the token from the client machine.

   Note: The common name must resolve to the IP address of the client machine, and port 80 on the client machine must be accessible to AppViewX.

   • A sample Certbot certificate enrollment command using HTTP challenge is as shown:

   ```
   certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /etc/avx-certbot/
   --config-dir /etc/avx-certbot/ --work-dir /etc/avx-certbot/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from
   AppViewX GUI>
   ```

2. **Using HTTP challenge when Apache server is running on Port 80**

   If the Apache server is already running on port 80 but is not available, Certbot's Apache plugin allows it to be used for challenge validation. To enable this functionality, a new folder must be created in the /etc directory. This directory will serve as the configuration, working, and log directory when using the **--apache plugin** option. For example, by creating a folder named **avx-certbot** within /etc and specifying it as a custom directory, this setup can be achieved..

   A sample command is as shown:

   ```
   certbot certonly --apache -d <domain_name> --preferred-challenges http -m <Email> --agree-tos --no-verify-ssl --server <ACME_URL>
   --config-dir /etc/avx-certbot/ --logs-dir /etc/avx-certbot/ --work-dir /etc/avx-certbot/
   ```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. **Using DNS challenge**

DNS-01 challenge: This challenge requires you to demonstrate control over the DNS for the domain name by inserting a specific value into a TXT record within that domain. Subsequently, AppViewX conducts a DNS query to verify the presence of the token in the domain's DNS records.

Refer to the following link to configure and use Certbot with different type of DNS servers: https://eff-certbot.readthedocs.io/

- **Default Challenge Validation (using default plugins)**

  This challenge requires demonstrating control over the DNS for a domain by adding a specific value to a TXT record within that domain. AppViewX then performs a DNS query to verify the presence of the token in the domain's DNS records.

  A sample command to do the challenge validation using the AWS route 53 server is as shown:

  ```
  certbot -vv certonly --preferred-challenges dns --dns-route53 -d <domain_name> --logs-dir /etc/avx-certbot/--config-dir /etc/avx-certbot/
  --work-dir/etc/avx-certbot/ -m <mail_id> --agree-tos --no-verify-ssl --server<ACME server endpoint URL fetched from AppViewX GUI>
  ```

  You must configure the credentials in Certbot to access the DNS servers. Refer to the following link to configure and use Certbot with different type of DNS servers: https://eff-certbot.readthedocs.io/en/stable/

- **DNS Challenge Validation (using AppViewX DNS plugin with Infoblox DNS Server)**

  This challenge requires demonstrating how AppViewX manages DNS for the domain by adding a specific value to a TXT record within it. AppViewX then performs a DNS query to verify the token's presence in the domain's DNS records. With the support of Platform Integration Hub, AppViewX will handle all tasks related to creating, searching for, and deleting TXT records in the DNS server.

  A sample command to do the AppViewX DNS Challenge Validation option is as shown:

  ```
  certbot certonly --dns-appviewx --dns-vendor infoblox --dns-server <Infoblox server name configured in appviewx> -d <Domain name> --logs-dir <logs dir>
  --config-dir <config dir> --work-dir <work dir> -m <mail id> --agree-tos --no-verify-ssl --eab-kid <key identifier> --eab-hmac-key <HMAC value> --server
  <acme url>
  ```

- **Enterprise Secure Challenge Validation**

  This challenge involves demonstrating how AppViewX manages DNS for a domain by querying the DNS A record to verify the presence of the client's IP address. This verification does not require DNS server credentials, as it only entails accessing the DNS A record for the specified domain.

  A sample command to do the AppViewX Enterprise Secure Challenge Validation option is as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
certbot certonly --dns-appviewx -d <Domain name> --logs-dir <logs_dir> --config-dir <config_dir> --work-dir <work_dir> --agree-tos --no-verify-ssl --eab-kid <key identifier> --eab-hmac-key <HMAC value> --server <acme_server_url>
```

Note: DNS Challenge Validation and Enterprise Secure Challenge Validation are only supported through the command-line interface (CLI) and not through the interactive script (execute.sh).

Re-enrolling Certbot using DNS-Based Challenge Validation

- **Default Challenge Validation**

```
certbot renew --no-verify-ssl --no-random-sleep-on-renew --eab-kid <key identifier> --eab-hmac-key <HMAC value> --config-dir <config dir for which renew should be triggered> --force-renewal
```

To automate renewal for Certbot through cron job, run:

```
(crontab -l ; echo "MM HH * * * /usr/bin/env bash -c 'source <certbot_folder/venv/bin/activate> && certbot renew --no-verify-ssl
 --no-random-sleep-on-renew
--config-dir <config_dir>'") | crontab -
```

- **DNS Challenge Validation**

```
certbot renew --dns-appviewx --dns-vendor infoblox --dns-server <Infoblox server name configured in appviewx> --no-verify-ssl
 --no-random-sleep-on-renew
--config-dir <config dir for which renew should be triggered> --eab-kid <key identifier> --eab-hmac-key <HMAC value> --force-renewal
```

To automate renewal for Certbot through cron job, run:

```
(crontab -l ; echo "MM HH * * * /usr/bin/env bash -c 'source <certbot_folder/venv/bin/activate> && certbot renew --dns-appviewx --dns-vendor infoblox
--dns-server <Infoblox server name configured in appviewx> --no-verify-ssl --no-random-sleep-on-renew --config-dir <config dir for which renew should be
 triggered> --eab-kid <key identifier> --eab-hmac-key <HMAC value> --force-renewal'") | crontab -
```

- **Enterprise Secure Challenge Validation**

```
certbot renew --dns-appviewx --no-verify-ssl --no-random-sleep-on-renew --config-dir <config dir for which renew should be triggered> --eab-kid <key identifier> --eab-hmac-key <HMAC value> --force-renewal
```

To automate renewal for Certbot through cron job, run:

```
(crontab -l ; echo "MM HH * * * /usr/bin/env bash -c 'source <certbot_folder/venv/bin/activate> && certbot renew --dns-appviewx --no-verify-ssl
--no-random-sleep-on-renew --config-dir <config dir for which renew should be triggered> --eab-kid <key identifier> --eab-hmac-key <HMAC value>
--force-renewal'") | crontab -
```

4. **Using Polling during Enrollment**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Polling can be activated when manual approval is configured for certificate generation. In this scenario, the client conducts polling for the certificate within a specified time frame, as determined by the configured parameters. If the certificate is approved before the polling duration expires, it is retrieved. To enable polling in the Certbot client, you may pass the parameters as mentioned:

Parameters	Type	Mandatory	Description
--retry-after	Integer	No	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 10]
--retry-frequency	Integer	No	The number of times for which the certificate is polled from the client side. [Default value : 20]

A sample command with **retry-after** as **5** and **retry-frequency** as **10** is as shown:

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /etc/avx-certbot/ --config-dir /etc/avx-certbot/
 --work-dir /etc/avx-certbot/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> --retry-after 5
 --retry-frequency 10
```

In this case, the certificate is polled 10 times with a 5-second interval for each polling attempt. Therefore, the polling process takes a total of 10 x 5 = 50 seconds to complete.

Note: To enable polling during the renewal process, it is important to include these parameters along with the renewal commands.

5. **Providing Custom and Certificate Attributes during Enrollment**

Certbot can be run with **custom attributes** allowing additional command line arguments. These arguments can include multiple name-value pairs, which are then included in the *Finalize Order* call along with the CSR. The values for these fields are provided as a JSON name/value pair, which can then be retrieved and mapped to the custom attributes in our application. This mapping enables including the custom attribute information in the certificate request for reporting.

A sample Certbot certificate enrollment command with custom attributes is as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /etc/avx-certbot/

--config-dir /etc/avx-certbot/ --work-dir /etc/avx-certbot/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX

GUI> --attributes "cust_id:123,name:appviewx" --attribute-type custom
```

This section covers the **attributes** and **attribute-type** parameters.

a. The **--attributes** field allows users to provide multiple attributes as a string with comma and colon separated values in the Certbot command. **Format:** name:AppViewX,city:Coimbatore

   The attributes field must adhere to the following guidelines:

   - The string must not be empty and must contain at least one name-value pair.
   - Multiple name-value pairs can be provided within the string separated by a comma.
   - Space is only allowed in the value field of the name-value pairs.
   - The attributes, after processing, will be sent as part of the payload in the finalize order call along with the CSR.

b. The **--attributes** field must be accompanied with the **--attribute-type** field that takes in one of the following inputs:

   - cert
   - custom
   - both

   i. When **attribute-type** is passed as **cert** the attributes from the (--attributes) field are taken as certificate attributes. An example of certificate attribute is:

   ```
   --attributes "id:1098,environment:development,Director:director_id" --attribute-type cert
   ```

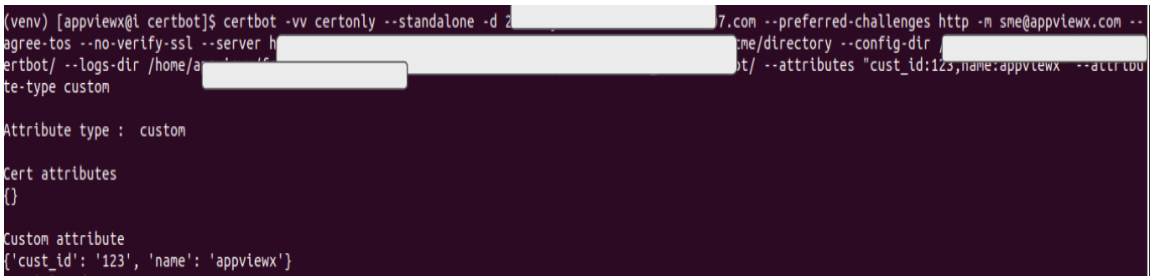
   The following image depicts how certificate attributes are defined in Certbot command:

   ii. When **attribute-type** is passed as **custom** the attributes from the (--attributes) field are taken as custom attributes. An example of certificate attribute is as follows:

   ```
   --attributes "cust_id:123,name:appviewx" --attribute-type custom
   ```

   The image shows how certificate attributes are defined in the Certbot command:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



iii. When **attribute-type** is passed as **both**, a JSON mapping is expected by the AppViewX Certbot. A new JSON file named attributesMapping.json needs to be created inside the Certbot folder. A sample JSON file is as shown:

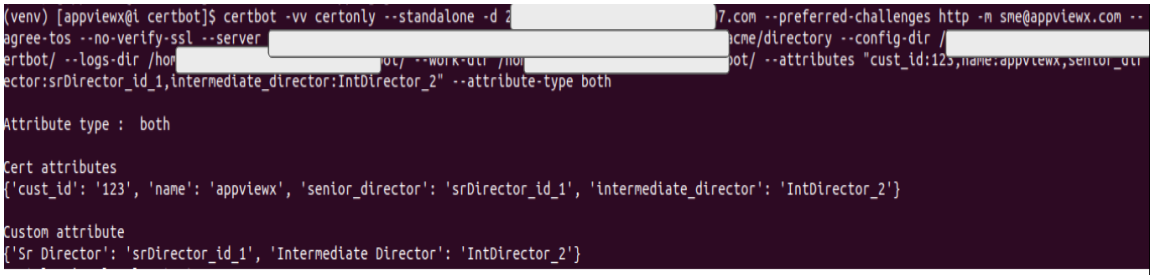
```
{
"senior_director" : "Sr Director",
"intermediate_director" : "Intermediate Director"
}
```

- The *key* [in the *key:value* pair from attributesMapping.json] refers to the certificate attribute key provided in the command, while the *value* corresponds to the custom attribute key where the value of the certificate attribute must be passed.
- The attributes passed as input are sent as certificate attributes. For attributes present in the attributesMapping.json, the mapped value is being used as attribute name and sent as custom attribute.

An example of custom attribute is as follows:

```
--attributes "cust_id:123,name:appviewx,senior_director:srDirector_id_1,intermediate_director:IntDirector_2" --attribute-type both
```

The image shows how certificate attributes are defined in Certbot command:



Note:

- The attributes are applicable only to *Method 1: Using Certbot Command Line*.
- If the attributes and attribute-type field are not specified in the Certbot command, normal flow of Certbot will work fine without any exceptions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. **Using EAB Credentials during Enrollment**

   A sample Certbot certificate enrollment command with external account binding enabled in the ACME server:

```
certbot -vv certonly --standalone --preferred-challenges http -d <domain_name> --logs-dir /etc/avx-certbot/

--config-dir /etc/avx-certbot/ --work-dir /etc/avx-certbot/ -m <mail_id> --agree-to s --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX

GUI> --eab-kid <Key identifier> --eab-hmac-key <MAC value>
```

   Note: This command is applicable only when the EAB algorithm is HS256. For other algorithms, use the cert_config.json file and adjust the configuration accordingly.

7. **Certbot - CSR and EAB Configuration**

   Providing CSR Parameters and EAB Fields

   The file named **cert_config_template.json** located in the Certbot directory is designed to facilitate the configuration of CSR and External Account Binding (EAB) fields. Renaming this file to **cert_config.json** and subsequently populating the required fields will ensure that these configurations are applied.

   CSR fields that can be provided:

   a. Subject fields:
      i. Organization
      ii. Organization unit
      iii. Country
      iv. State
      v. Locality
   b. Hashing algorithm
   c. RSA Key-Size
   d. key type
   e. elliptic curve details

   EAB fields that can be provided:

   a. EAB HMAC
   b. EAB KID
   c. EAB Algorithm

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- EAB details can be provided via Certbot command parameters or a cert_config.json file. The Certbot command only supports HS256. Other EAB algorithms require the cert_config.json file.
- The cert_config.json file contains key-value pairs for all subject fields. If any of these fields are not required, the corresponding key-value pair can be deleted from thecert_config.json.

A sample JSON is as follows:

```
{
"csr_params": {
        "organization" : "AVX",
        "organization_unit" : "AVX_IOT",
        "country" : "IN",
        "state" : "TN",
        "locality" : "CBE",
        "hashing_algorithm":"SHA512",
        "rsa_key_size": "4096",
        "key_type":"rsa",
        "elliptic_curve":""
        },
"eab": {
        "kid":"",
        "mac":"",
        "alg":""
}
```

Json keys	Expected Input	Comments
csr_params:organization **csr_params:organization_unit** **csr_params:country** **csr_params:state**	String	Choose the appropriate subject fields for the CSR.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

csr_params:Locality		
csr_params:hashing_algorithm	<Hashing_Algorithm>	Choose the appropriate hashing algorithm [SHA256,SHA384 & SHA512]
csr_params:rsa_key_size	<RSA_keysize> (String)	Default value : “2048” The size of the private key to use for the certificate. For RSA keys, specify a number between 2048-4096 (divisible by 128) [Provide this field only when key_type is set to “rsa”]
csr_params:key_type	Possible values : [“rsa”, “ecdsa”] (String)	Default value : “rsa” Provide the key type which can be used for private key generation.
csr_params:elliptic_curve	Possible values : [“secp256r1” , “secp384r1”, “secp521r1”] (String)	Default value : “secp256r1” The type of elliptic curve can be specified here. [Provide this field only when key_type is set to “ecdsa”]
eab:kid	<value_of_EAB_KID>	Key Identifier for External Account Binding (Optional).
eab:hmac	<value_of_EAB_HMAC_KEY>	HMAC key for External Account Binding (Optional).
eab:alg	HS256/HS384/HS512	Default value : “HS256”

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

		Signature Algorithm for External Account Binding.

Note: When a certificate is initially created with **key_type** set to rsa and needs to be changed or renewed to ecdsa, you must use the **--key-type ecdsa** option along with **--cert-name** on the command line during the certificate creation or renewal process.

Example: `certbot renew --key-type ecdsa --cert-name example.com --force-renewal`

Enrolling Certificates with DNS Validation using Azure Plugin

Prerequisite

Set up Azure Credentials

1. Create the azure.ini file in any path that Certbot can access, for example, you can use /opt/.secrets/azure.ini as config file for Azure credentials.
2. Add the following template config in /opt/.secrets/azure.ini:
   - dns_azure_sp_client_id = xxx-xxx-xxx-xx
   - dns_azure_sp_client_secret = xxx-xxx-xxx-xx
   - dns_azure_tenant_id = xxxx-xxx-xxx-xx
   - dns_azure_environment = "AzurePublicCloud"
   - dns_azure_zone1 = <zoneName>:/subscriptions/<subscription_id>/resourceGroups/<resouce_group_name>

Note: Multiple DNS zones can be added in the following variable format, **dns_azure_zone(X)**, where X denotes incremental integers.

Enrolling Certificates for Public DNS Zone

```
certbot certonly --authenticator dns-azure --preferred-challenges dns  \
--dns-azure-config /opt/.secrets/azure.ini \
--logs-dir <logs_dir> \
--config-dir <config_dir> \
--work-dir <work_dir> \
-d <FQDN_NAME_FOR_CERTIFICATE> \
-m <email_id> --agree-tos \
--server <ACME_SERVER_URL> \
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
--eab-kid <EAB_KEY> \
--eab-hmac-key <EAB_HMAC_KEY>
```

Enrolling Certificates for Private DNS Zone

```
certbot certonly --authenticator dns-azure --preferred-challenges dns \
--dns-azure-config /opt/.secrets/azure.ini \
--logs-dir <logs_dir> \
--config-dir <config_dir> \
--work-dir <work_dir> \
-d <FQDN_NAME_FOR_CERTIFICATE> \
-m <email_id> --agree-tos \
--server <ACME_SERVER_URL> \
--eab-kid <EAB_KEY> \
--eab-hmac-key <EAB_HMAC_KEY
```

Method 2: Using AppViewX Certbot User-Friendly Script

Activating Virtual Environment

With the AppViewX Certbot user-friendly script, you can run commands to perform enroll, renew, and revoke certificate actions by activating the virtual environment as described in this section.

1. Go to the Certbot folder and open the terminal from that path.

   ```
   cd /path/to/file/AppViewX_ACME_Certbot_Client
   ```

2. Run:

   ```
   ./execute.sh
   ```

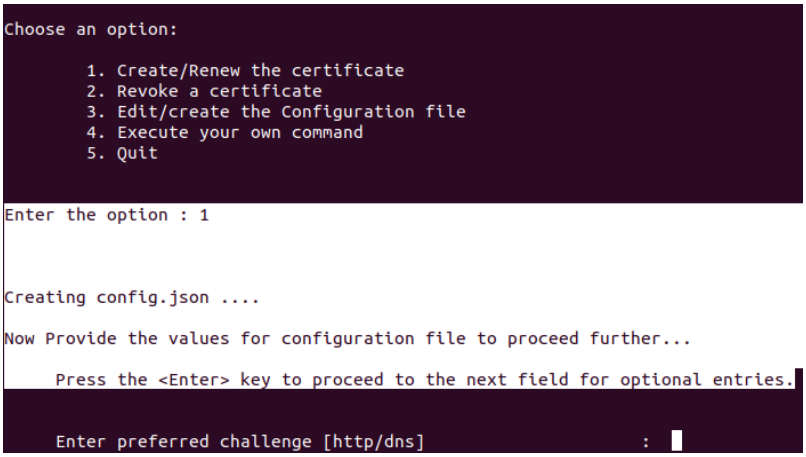
   Note: You must log on as a root user (`sudo -i`) before running the `execute.sh` file.

   Once Certbot is ready to use, it displays the following options:

   - Create/Renew a certificate
   - Revoke a certificate
   - Edit/create the Configuration file
   - Execute your own command
   - Quit

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. When using the user prompt for the first time, you are automatically redirected to option 3 even if you select option 1 or 2. This is to fill all the parameters that are required for the command to be run as shown in the next sections.



All the parameters are stored in a JSON config file (/<filepath>/AppViewX_ACME_Certbot_Client/certbot/config.json) created by AppViewX. A sample of the configuration being updated is as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
Choose an option:

        1. Create/Renew the certificate
        2. Revoke a certificate
        3. Edit/create the Configuration file
        4. Execute your own command
        5. Quit


Enter the option : 1



Creating config.json ....
Now Provide the values for configuration file to proceed further...

     Enter preferred_challenges [http/dns]                :  http
     Enter server specification [standalone/apache]       :  standalone
     Enter logs directory                                 :  /home/appviewx/certbot/certbot_certs/
     Enter config directory                               :  /home/appviewx/certbot/certbot_certs/
     Enter work directory                                 :  /home/appviewx/certbot/certbot_certs/
     Enter email address                                  :  example@appviewx.com
     Enter server URL                                     :  <ACME server endpoint URL fetched from Appviewx GUI>
     Enter whether agreeing to terms of services [y/n]    :  y
     Enter whether need to verify the SSL [y/n]           :  y
     Enter eab_kid [optional]                             :
     Enter eab_hmac_key [optional]                        :
     Enter Key Type [rsa/ecdsa]                           :  rsa
     Enter RSA key size [1024/2048/3072/4096]             :  2048


Inputs saved to Configuration file
```

```
Inputs saved to Configuration file
Creating/Renewing a cert option selected....


***************************
CONFIGURATION FILE
***************************
{
  "server": "standalone",
  "preferred_challenges": "http",
  "logs_dir": "/home/appviewx/certbot/certbot_certs/",
  "config_dir": "/home/appviewx/certbot/certbot_certs/",
  "work_dir": "/home/appviewx/certbot/certbot_certs/",
  "email": "example@appviewx.com",
  "server_url": "<ACME server endpoint URL fetched from Appviewx GUI>",
  "agree_tos": "y",
  "verify_ssl": "y",
  "eab_kid": "",
  "eab_hmac_key": "",
  "key_type": "rsa",
  "rsa_key_size": "2048",
  "elliptic_curve": ""
}


The above are the present values of the configuration file.

        If you want to  change them, Enter (1) to exit and use Edit Configuration option..
        Else press <Enter> to continue with the old value..


Enter your option :
```

Enrolling or Renewing Certificate using Interactive Script

1. To create/renew a certificate enter 1.

   A JSON configuration file is displayed that has the fields with previously saved values.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
Enter the option : 1


Creating/Renewing a cert option selected....


*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :
```

2. To proceed with the displayed values (already existing values in the JSON configuration file), press the **Enter** key.
3. Enter the *domain name* for which the certificate needs to be enrolled.

```
*****************************************************************
The following are the recently configured values provided by you.
*****************************************************************

The Preferred Challenges selected is           : http
The Logs Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is          : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is            : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                  : example@gmail.com
The Server URL provided is                     : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                      : y
The EAB Kid value provided is                  :
The EAB HMAC Key provided is                   :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :


        Enter the domain names for which the certificate needs to be created     : exampledomain.com


certbot -vv certonly -d exampledomain.com --null --preferred-challenges http --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /ho
me/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m example@gmail.com --agree-tos --server <ACME server end
point URL fetched from AppViewX GUI>
```

The process continues and the certificate from the specified path is created.

Revoking Certificate

Certificate revocation can be performed in two ways: either by using the certificate path or by using the certificate name:

- **Cert Path**

```
certbot revoke --cert-path <Path-to-fullchain.pem> --config-dir <Certbot-config-directory> --work-dir <Certbot-work-directory> -m <mail-id> --no-verify-ssl

 --agree-tos --server <ACME server endpoint URL fetched from AppViewX GUI>
```

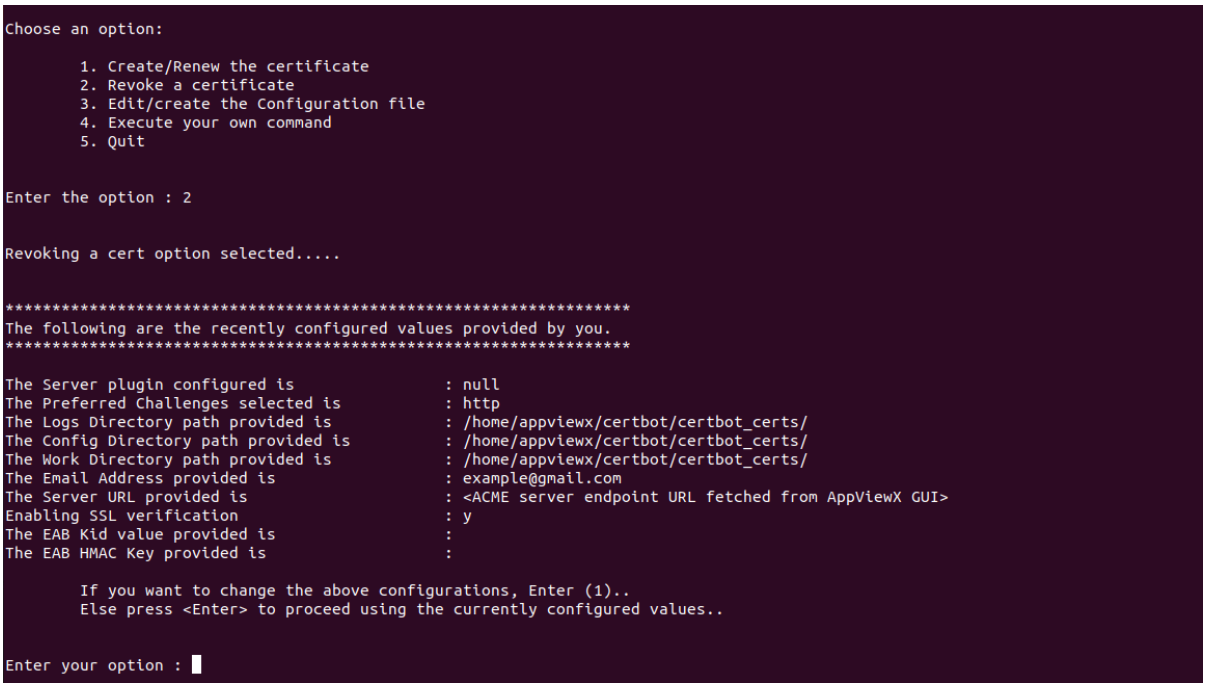
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Cert Name**

```
certbot revoke --cert-name <domain_name> --config-dir <Certbot-config-directory> --work-dir <Certbot-work-directory> -m <mail-id> --no-verify-ssl --agree-tos
 --server <ACME server endpoint URL fetched from AppViewX GUI>
```

1. To revoke a certificate, enter 2.

   A JSON configuration file is displayed that has the fields with previously saved values.



2. To proceed with the displayed values (already existing values in the JSON configuration file), press the **Enter** key.
3. Enter the *certificate path* for which the certificate needs to be revoked.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
Revoking a cert option selected.....


****************************************************************
The following are the recently configured values provided by you.
****************************************************************

The Server plugin configured is               : null
The Preferred Challenges selected is          : http
The Logs Directory path provided is           : /home/appviewx/certbot/certbot_certs/
The Config Directory path provided is         : /home/appviewx/certbot/certbot_certs/
The Work Directory path provided is           : /home/appviewx/certbot/certbot_certs/
The Email Address provided is                 : example@gmail.com
The Server URL provided is                    : <ACME server endpoint URL fetched from AppViewX GUI>
Enabling SSL verification                     : y
The EAB Kid value provided is                 :
The EAB HMAC Key provided is                  :

        If you want to change the above configurations, Enter (1)..
        Else press <Enter> to proceed using the currently configured values..


Enter your option :


        Enter the Certificate Path                                          : /home/path_to_the_cert_that_needs_to_be_revoked


certbot -vv revoke --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appvie
wx/certbot/certbot_certs/ -m example@gmail.com --agree-tos --server <ACME server endpoint URL fetched from AppViewX GUI> --cert-path /home/pat
h_to_the_cert_that_needs_to_be_revoked
```

The process continues and the certificate from the specified path is revoked.

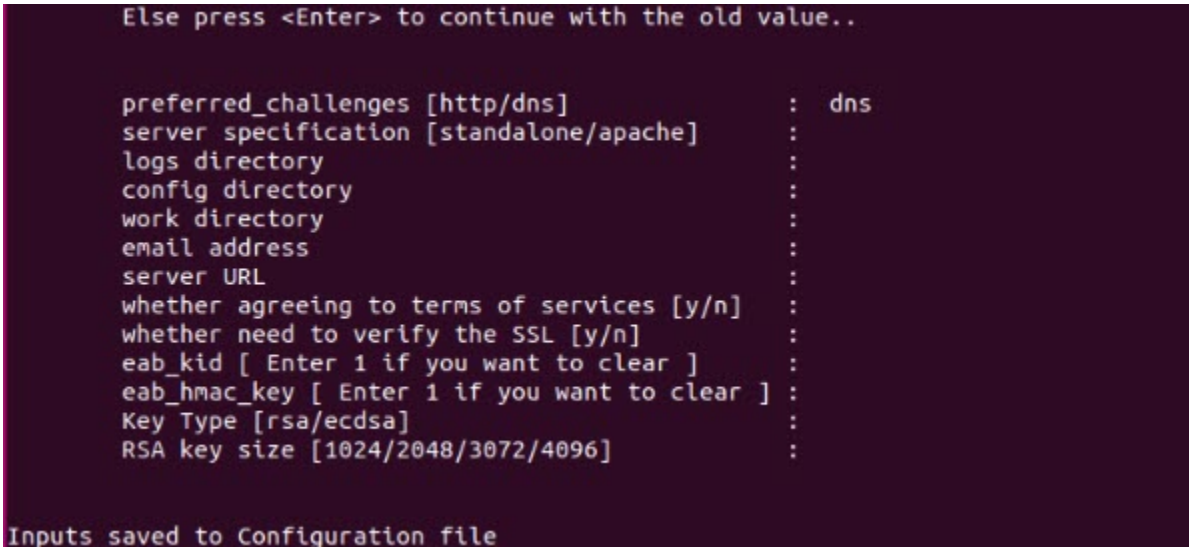
Creating or Editing Configuration File

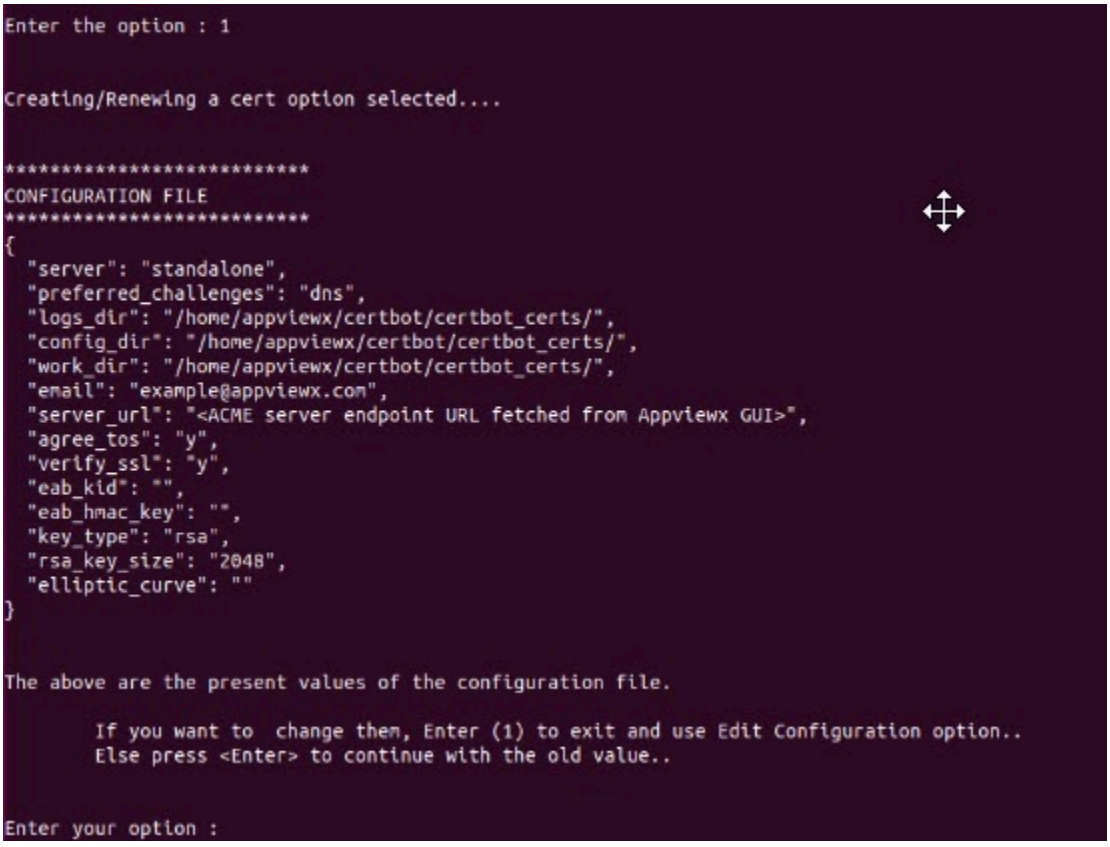
1. To edit the displayed values (already existing values in the JSON configuration file), enter `1` to exit and then enter `3` to edit the configuration file.

```
Choose an option:

        1. Create/Renew the certificate
        2. Revoke a certificate
        3. Edit/create the Configuration file
        4. Execute your own command
        5. Quit


Enter the option : 3


Creating or Editing Configuration file Option is selected

{
  "server": "standalone",
  "preferred_challenges": "http",
  "logs_dir": "/home/appviewx/certbot/certbot_certs/",
  "config_dir": "/home/appviewx/certbot/certbot_certs/",
  "work_dir": "/home/appviewx/certbot/certbot_certs/",
  "email": "example@appviewx.com",
  "server_url": "<ACME server endpoint URL fetched from Appviewx GUI>",
  "agree_tos": "y",
  "verify_ssl": "y",
  "eab_kid": "",
  "eab_hmac_key": "",
  "key_type": "rsa",
  "rsa_key_size": "2048",
  "elliptic_curve": ""
}


The above are the present values of the configuration file.
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. As an example, change the preferred_challenges value to DNS. Enter the DNS value.

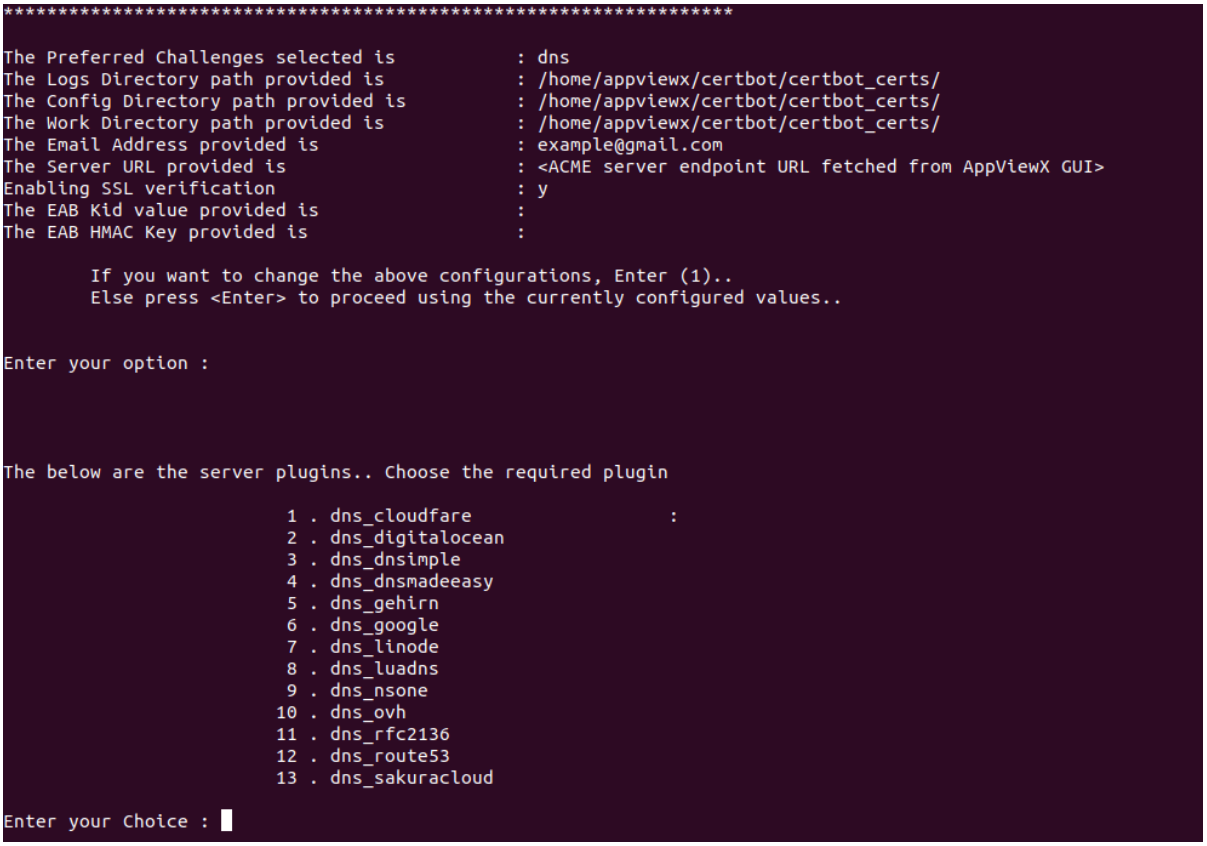




Note: If you want to proceed with the displayed values (already existing values in the JSON configuration file), press the **Enter** key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Select and enter the DNS server among all the list DNS servers supported by Certbot.



4. Enter the credentials of the DNS server such that the command is run accordingly.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
The below are the server plugins.. Choose the required plugin

                          1 . dns_cloudfare                 :
                          2 . dns_digitalocean
                          3 . dns_dnsimple
                          4 . dns_dnsmadeeasy
                          5 . dns_gehirn
                          6 . dns_google
                          7 . dns_linode
                          8 . dns_luadns
                          9 . dns_nsone
                         10 . dns_ovh
                         11 . dns_rfc2136
                         12 . dns_route53
                         13 . dns_sakuracloud

Enter your Choice : 12


dns_route53 option selected....



**************************
ROUTE53 CREDENTIALS FILE
**************************
[default]
aws_access_key_id=<enter_valid_aws_access_key_id>
aws_secret_access_key=<enter_valid_aws_secret_access_key>


The above are the present values of the credentials file for dns_route53..
        If you want to  change them, Enter (1) to edit credentials..
        Else press <Enter> to continue with the old value..


Enter your option :
```

a. This process involves creating a secrets folder (in /path/to/file/AppViewX_ACME_Certbot_Client/certbot) that stores all the credential files with token/credentials) of all the DNS servers supported. The token/credentials are provided by the users.

```
**************************
ROUTE53 CREDENTIALS FILE
**************************
[default]
aws_access_key_id=<enter_valid_aws_access_key_id>
aws_secret_access_key=<enter_valid_aws_secret_access_key>


The above are the present values of the credentials file for dns_route53..
        If you want to  change them, Enter (1) to edit credentials..
        Else press <Enter> to continue with the old value..


Enter your option :


        Enter the domain names for which the certificate needs to be created     : exampledomain.com


certbot -vv certonly -d exampledomain.com --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-d
ir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m example@gmail.com --agree-tos --server <ACME serv
er endpoint URL fetched from AppViewX GUI>
```

b. Once the credentials file is created, you can continue with the existing credentials file values or modify them to proceed with the new values by using the prompted guidance on the screen.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

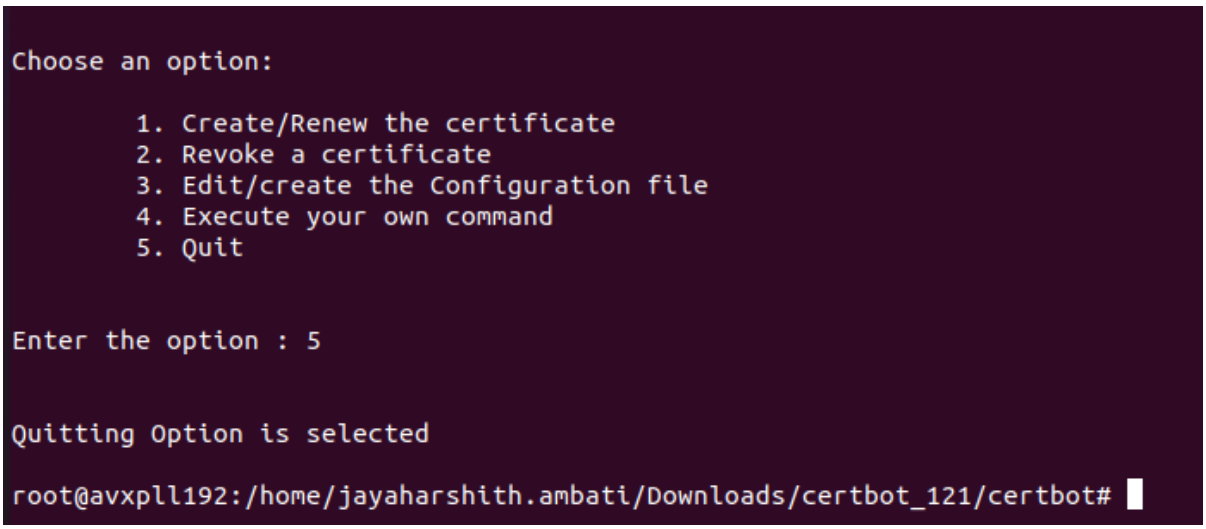
c. Only for DNS route 53, the Certbot application stores the required credentials/tokens in the /root/.aws/credentials path. Initially it checks for the .aws folder in /root/.aws path; if not found, it creates a .aws folder and a credentials file inside it.

d. If the .aws folder and credentials file is found in the root directory, the values are updated per the inputs provided. You can proceed with the existing values or with new values by editing the credentials file.

e. For all the remaining DNS servers, inputs (tokens/keys) for the credentials file are taken from the user. Once the credentials file is created, you can continue with existing credentials file values or modify and proceed with the new values by using the prompted guidance on the screen.

5. To run your own commands manually, select/enter option 4.

6. After the selected option's functionality is done, all the five options are displayed each time in the same virtual environment until the quit option 5 is selected.



Points to Remember

1. Preferred challenges must either be given as **http** or **dns** only.
2. **Agree to terms of services** and **verify ssl** fields must either be given as *y (yes) or n (no)*.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the **verify ssl** field is enabled (when the **verify ssl** field is given as **y**), see Section, *Adding Custom CA Certificates to Trust Store*.

3. Provide valid **email address** and **domain names**.
4. The **eab_kid** and **eab_hmac_key** fields.
   a. These are optional fields, so you can proceed by pressing the **Enter** key without providing the values.
   b. The values can be cleared from the JSON configuration file by selecting **1** at the time of editing the configuration file.
5. During the configuration process, you can also specify the key type (RSA/ECDSA) and key size. Depending on the key type provided, input for RSA key size or elliptic curve details will be requested.
6. You can enter new values when option 3 (Edit/Create the Configuration file) is selected. Select fields can be edited/updated. For all retaining old values, press the **Enter** key.
7. The **domain name** field:
   a. Provide a *single domain name* to acquire a certificate for a particular domain.
   b. Provide comma separated *multiple domain names* to acquire a certificate for all the given domains.
   c. *Wildcard certificates* can be acquired by providing input for a particular domain.
8. The **jq** package.
   a. Having the **jq** package installed on your system is a prerequisite (must) to proceed with the user prompt guidance provided by the script. Ignore this step if it is not compatible with your environment.
   b. After running the execute.sh script, the system checks if the **jq** package is installed on your system.
   c. If it is not installed on your system and you want to access the user prompt guidance, click 1 to proceed with the installation.
   d. You may also click 2 to exit and run your own command manually in the same virtual environment created by execute.sh script.

Best Practices

- For auto-enrollment, create a separate certificate group and CA policy in AppViewX.
- Enable auto-renewal in the AppViewX policy.
- During policy creation, select only the required bit-length (minimum 2048-bit).
- It is recommended to use EAB settings to ensure that only the intended clients are able to generate certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting

Accessing the ACME Logs

1. Access the terminal window.
2. Go to <Installed_Path>/logs directory and find the name format with <avxgw-HTTPS-<yyyy-mm-dd>.log>, for example, <avxgw-HTTPS-2021-03-17.log>.
   - If the file size exceeds 100MB, it will be rolled over and the latest logs will be available in the latest file named with an incrementing counter starting from 1 such as avxgw-HTTPS-<yyyy-mm-dd>.<incrementing_counter>.log, for example, <avxgw-HTTPS- 2021-03-17.1.log>.
   - ACME plugin logs:

     </home/appviewx/appviewx/logs/avx-vendor-cert-acme-agent-<pod_name>.log>

Client-side Errors

General Errors

Sr. No.	Error Message	Description	Troubleshooting
1	Challenge failed for domain testav.appviewx.com Notifying user: Certbot failed to authenticate some domains (authenticator: standalone). Some challenges have failed.	HTTP challenge validation failed.	Make a DNS entry.
2	Unable to locate credentials To use certbot-dns-route53, configure credentials as described at https://boto3.readthedocs.io/en/latest/guide/configuration.html#best-practices-for-configuring-credentials and add the necessary permissions for Route53 access.	DNS challenge validation failed. Invalid credentials were utilized for DNS challenge validation.	Ensure the credentials in the credentials file are valid.
3	An error occurred (InvalidClientTokenId) when calling the ListHostedZones operation: The security token included in the request is invalid.	DNS challenge validation failed. The required credentials	Ensure the credentials file with the required credentials is

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
	To use certbot-dns-route53, configure credentials as described at https://boto3.readthedocs.io/en/latest/guide/configuration.html#best-practices-for-configuring-credentials and add the necessary permissions for Route53 access.	file for DNS challenge validation is missing.	present and valid.
4	{"appStatusCode":"AVX_GW_009","message":"Resource not found, reason - Invalid apiid"} An unexpected error occurred: acme.messages.Error: about:blank	The provided endpoint url is improperly configured.	Ensure that the endpoint URL is valid.
5	An unexpected error occurred: requests.exceptions.ConnectionError: HTTPSConnectionPool(host='<hostname/ipaddress>', port=31443): Max retries exceeded with url: / avxapi/acmeTest/acme/directory (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f3ddc7d7970>: Failed to establish a new connection: [Errno -2] Name or service not known'))	The user interface has an incorrect configuration for the endpoint.	Verify that the user interface is correctly set up with the appropriate endpoint configuration.
6	An unexpected error occurred: requests.exceptions.InvalidURL: Failed to parse: https://<hostname/ipaddress>:314423/avxapi/acmeTest/ acme/ directory	The provided endpoint URL contains an invalid port number. **(or)** Network configuration regulations, firewall rules that prevent access	Ensure that the port specified in the endpoint URL is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
		to the required port.	
7	An unexpected error occurred: ValueError: Requesting <hostname/ ipaddress>.appviewx.net/avxapi: Connection refused	The user interface has an incorrect configuration for the endpoint port.	Verify that the port is properly configured within the user interface.
8	Client with the currently selected authenticator does not support any combination of challenges that will satisfy the CA. You may need to use an authenticator plugin that can do challenges over DNS.	The challenge type set on the server side is HTTP, but the request sent from the client was configured using the DNS challenge.	The request made from the client must be configured to use HTTP challenge.
9	Client with the currently selected authenticator does not support any combination of challenges that will satisfy the CA.	The challenge type set on the server side is DNS, but the request sent from the client was configured using the HTTP challenge.	The request made from the client must be configured to use DNS challenge.
10	Notifying user: Certbot failed to authenticate some domains (authenticator: standalone). Some challenges have failed.	Obtaining wildcard certificates through HTTP challenge validation.	Obtain wildcard certificates exclusively through the DNS challenge validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
11	Certificate did not match expected hostname: <hostname/ipaddress> Certificate: {'subject': ((('commonName', 'comman_name'),),), … An unexpected error occurred: requests.exceptions.SSLError: HTTPSConnectionPool(host='<hostname/ipaddress>', port=31443): Max retries exceeded with url: /avxapi/acmeTest/acme/directory (Caused by SSLError(SSLCertVerificationError("hostname '<hostname/ipaddress>' doesn't match 'serverside_configured_<hostname/ipaddress>'")))	Setting up the ACME endpoint with an IP address to facilitate SSL verification.	Configure the ACME end point with FQDN (Fully Qualified Domain Name) instead of IP address for SSL verification.
12	Another instance of Certbot is already running	Attempting to launch Certbot while another instance is already active, or when the Certbot process is forcefully terminated.	Terminate the Certbot process that ended abruptly, or terminate the currently active Certbot process. Use the command: **pkill -9 certbot**
13	The following error was encountered: [Errno 13] Permission denied: '/home/jayaharshith.ambati/certbotagent.log' Either run as root, or set --config-dir, --work-dir, and --logs-dir to writeable paths.	In cases where administrative privileges are not granted.	Ensure administrative privileges (sudo access) is provided to run Certbot.
14	Too many flags setting configurators/installers/authenticators 'standalone' -> 'dns-route53'	Utilizing both the standalone plugin and the	At any given time, we have the option to select only one

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
		DNS plugin (DNS Route 53).	plugin, which means we can choose either --standalone or --dns-route-53, but not both simultaneously.
15	IndexError: list index out of range	When there is a lack of input for at least one custom attribute.	Using custom attributes requires at least one input to be provided.
16	key, value = attr.split(':') ValueError: not enough values to unpack (expected 2, got 1)	When custom attributes are not provided in the format of key-value pairs.	Custom attributes need to be provided in the form of key-value pairs.
17	An unexpected error occurred: The "externalAccountBinding.protected" field is invalid.:: kid is invalid	When the **--eab-kid** value is altered or provided incorrectly, an error occurs.	Please ensure that the provided **--eab-kid** value matches the configuration set in the AppViewX UI.
18	{"detail":"The \"externalAccountBinding.signature\" field is invalid.","type":"urn:ietf:params:acme:error:invalidExternalAccountBindingParameters(signature)"} An unexpected error occurred: The "externalAccountBinding.signature" field is invalid.	When the **--eab-hmac-key** value is altered or provided incorrectly, an error occurs.	Ensure that the provided **--eab-hmac-key** value matches the configuration set in the AppViewX UI.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
19	An e-mail address or --register-unsafely-without-email must be provided.	Email address is not provided in the command.	Ensure that a valid email address is provided in the command.
20	An unexpected error occurred: requests.exceptions.SSLError: HTTPSConnectionPool(host='<hostname/ipaddress>', port=31443): Max retries exceeded with url: /avxapi/acmeTest/acme/directory (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1131)')))	SSL Verification failed.	To activate SSL verification, it is essential to confirm that the server trust chain certificates exist within the machine's trust store. To achieve this, you can refer to the instructions outlined in the Section, *Setting the Custom CA Certificate Path Manually.*
21	Could not bind TCP port 80 because it is already in use by another process on this system (such as a web server). Please stop the program in question and then try again.	Port 80 is not accessible.	Stop any process running on port 80 as the Linux machine should be accessible from AppViewX CC (port 80)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
			for HTTP-01 challenge.
22	Self DNS Challenge token validation/IP Validation option is selected but EAB details/Allowed domains are not configured for the agent settings.	When AppViewX **DNS Challenge** or **Enterprise Secure Challenge Validations** is selected but **Allowed Domains** or EAB details are not provided from the ACME client, you get this error.	1. Provide valid domains under the **Allowed Domains** field. 2. Enable either **Static EAB** or **Dynamic EAB credentials**.
23	DNS Challenge validation failed. IP Options are not selected for agent settings. Allowed options are STRICT, ANY, NONE.	If Enterprise Secure Challenge type other than **Secure, Any, Ignore** is selected in the ACME Settings.	Select any one of the following under Enterprise Secure Challenge options: **Secure, Any, Ignore.**
24	DNS Challenge validation failed. ACME DNS challenge verification via DNS A record failed. For STRICT Option IP didn't Match.	If the **Secure** option is selected under **Enterprise Secure Challenge** type and the ACME client's IP address does not match with	Make sure that the DNS A record of the requesting domain contains the same IP address as the ACME client's IP address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
		the available DNS A record for the particular domain.	
25	The requested account is not available.	Whenever the EAB configurations are switched between Static and Dynamic, or when the EAB algorithm is changed, the ACME account will be cleared from the ACME server. As a result, the user may encounter this error.	Clear the accounts folder located under the config directory. This will remove the accounts from the client side as well, causing Certbot to treat it as a new account and create it accordingly.
26	DNS Challenge validation failed. ACME DNS challenge verification via DNS A record failed. For STRICT Option there are more IP address entries in DNS A Record.	If the **Secure** option is selected under **Enterprise Secure Challenge** type and the DNS A record for the requesting domain is fetched with more than one IP address.	Make sure that the DNS A record of the requesting domain contains only one IP address, which is the same as the ACME client's IP address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
27	DNS Challenge validation failed. No DNS A records are found to validate ANY type.	If the **ANY** option is selected under **Enterprise Secure Challenge** type and the DNS A records for the requesting domain are fetched in which none of the IP address matches with the ACME client's IP address.	Make sure that the DNSA records of the requesting domain contains any one IP address, which is the same as the ACME client's IP address.
28	DNS Challenge validation failed. DNS A record for the domain <domain name> is not available.	When AppViewX is not able to obtain the DNS A records for the requesting domain.	• Check if the DNS Server is reachable from AppViewX to resolve and obtain the DNS A records of the requesting domain. • Check if the provided DNS server hostname is proper to resolve

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
			and obtain the DNS A records.
29	DNS Challenge validation failed. Error while executing Create/Delete record operation.	1. When AppViewX is not able to reach the DNS server for creating DNS TXT for the requesting domain. 2. When there are errors while performing creation or deletion of DNS TXT records in the DNS server.	1. Check if the DNS server is reachable from AppViewX. 2. Check AppViewX logs for detailed errors regarding creation and deletion of errors.
30	Some challenges have failed.[And acme logs show that403 Forbidden]	Config, work, and logs directory do not have sufficient permissions.	Provide chmod 755 permission to the logs/ config and work directories.
31	Could not reverse map the HTTPS VirtualHost to the original	The virtual host server names for ports 80 and 443 are different.	Change the port 80 virtual host's server name to match the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sr. No.	Error Message	Description	Troubleshooting
			domain name or certificate common name.

Other General Errors

Sr.No.	Error and Cause	Solution
1	Firewall blockage connectivity error A "firewall blockage connectivity error" when using Certbot typically occurs when the Certbot client is unable to establish a connection to external servers due to network restrictions or firewall rules. This can prevent Certbot from successfully completing the domain ownership verification process required to obtain SSL/TLS certificates.	Ensure that network restrictions or firewall rules are configured as necessary.
2	The port to contact with Acme End point is not accessible error	**Firewall Rules:** If your server is behind a firewall or network security appliance, ensure that the necessary ports (typically ports 80 and 443) are allowed for inbound and outbound connections. ACME challenges often use these ports to verify domain ownership. **Blocked Ports:** Some hosting providers or network environments might block certain ports, including ports 80 and 443, to prevent web services from being accessible. Verify that the necessary ports are open and accessible.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Errors due to extra arguments

Errors are also encountered if any extra arguments, other than supported arguments are given in the Certbot command. They are as follows:

1. **Sample command:** `certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> -`

   Error: certbot: error: unrecognized arguments

2. **Sample command:** `certbot certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> cert`

   Error: certbot: error: unrecognized arguments: cert

3. **Sample command:** `certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> -cert`

   Error: certbot: error: Unable to open config file: ert. Error: No such file or directory

4. **Sample command:** `certbot -vv certonly -d sampledomain.info --preferred-challenges dns --dns-route53 --logs-dir /home/appviewx/certbot/certbot_certs/ --config-dir /home/appviewx/certbot/certbot_certs/ --work-dir /home/appviewx/certbot/certbot_certs/ -m <mail_id> --agree-tos --no-verify-ssl --server <ACME server endpoint URL fetched from AppViewX GUI> -test`

   Error: certbot: error: argument -t/--text: ignored explicit argument 'est'

Glossary

Keywords used in Certbot Commands

Keyword	Expected Input	Comments
-v, --verbose	NA	This flag can be used multiple times to incrementally increase the verbosity of the output, for example, -vvv. (default: 0)
(default) run	NA	Obtain and install a certificate in your current web server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Keywords used in Certbot Commands (continued)

Keyword	Expected Input	Comments
certonly	NA	Obtain or renew a certificate, but do not install it.
--standalone	NA	Run a standalone web server for authentication.
-d (Domain)	<domain1.com> or <domain2.com>, <domain3.com>, <domain4.com>	Comma-separated list of domains to obtain a certificate for.
--preferred-challenges	http/dns	A sorted, comma delimited list of the preferred challenge to use during authorization with the most preferred challenge listed first. The default value of preferred challenges is an **empty list.**
--config-dir	<path_to_config_directory>	The config directory contains Certbot's configuration files, including information about the certificates, domains, renewal settings, and more. It is where Certbot stores its persistent configuration data. Certbot keeps track of the certificates it manages, their associated options, and renewal schedules in this directory. Custom configuration directory path (**default**: /etc/letsencrypt).
--work-dir	<path_to_work_directory>	The work directory is used by Certbot to store temporary files and data while it performs operations like certificate issuance and renewal. This directory is where Certbot creates and stores temporary

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Keywords used in Certbot Commands (continued)

Keyword	Expected Input	Comments
		challenges required for domain ownership verification during the certificate issuance process. It is a workspace for Certbot's internal processes. Custom working directory path (**default**: /var/lib/letsencrypt).
--logs-dir	<path_to_logs_directory>	The logs directory contains log files that record the activities and events related to Certbot's operations. These logs can provide valuable information for troubleshooting issues and understanding the certificate issuance and renewal process. Logs include details about challenges, certificate renewals, errors, and more. Custom logs directory path (**default**: /var/log/letsencrypt).
-m	<example1@gmail.com> or <example2@gmail.com>, <example3@gmail.com>	Email used for registration and recovery contact. Use commas to register multiple emails. Email address for important account notifications.
--agree-tos	NA	Agree to the ACME server's Subscriber Agreement.
--no-verify-ssl	NA	Disable verification of the ACME server's certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Keywords used in Certbot Commands (continued)

Keyword	Expected Input	Comments
--server	<Acme Server Endpoint URL fetched from AppViewX GUI>	ACME Directory Resource URI. (default: https://acme-v02.api.letsencrypt.org/directory)
--eab-kid EAB_KID	<value_of_EAB_KID>	Key Identifier for External Account Binding (Optional).
--eab-hmac-key EAB_HMAC_KEY	<value_of_EAB_HMAC_KEY>	HMAC key for External Account Binding (Optional).
revoke	NA	Used for revoking a certificate.
--cert-path	<path_to_certificate> Example: /home/appviewx/certbot/certbot_certs/live/certbot.appviewx.info/fullchain.pem	Path to where certificate is saved (with certonly --csr), installed from, or revoked (default: None)
--dns-route53	NA	Obtain certificates using a DNS TXT record (if you are using Route53 for DNS). (default: False).
--attributes	Sample input: **"name:AppViewX,city:Coimbatore"** The string should not be empty and must contain at least one name-value pair.	The --attributes field allows users to provide multiple attributes as a string with comma and colon separated values in the Certbot command. [It is optional, but **--attributes** field must be accompanied with the **--attribute-type** field.]
--attribute-type	Any one of the following : **cert/custom/both**	Takes in one of the following inputs **cert/custom/both**. [It is optional, but must be included when **--attributes** is passed.]

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Keywords used in Certbot Commands (continued)

Keyword	Expected Input	Comments
--retry-after	Integer	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 10]
--retry-frequency	Integer	The number of times for which the certificate is polled from the client side. [Default value : 20]

Configuring AppViewX Posh-ACME Client

Getting Started

Prerequisites

- The AppViewX server/cloud connector must be bound with a valid certificate. See Section, *Binding Custom Certificate to Gateway in Cloud Connector*.
- Root user permissions for setup process in Linux.
- Admin privileges are required during setup and runtime in Windows.
- A proper DNS entry for the services in the DNS server.
- A valid ACME endpoint must be configured on the AppViewX GUI.
- To enable client connections, it is essential to have port 31443 open for on-premise deployment and port 30020 (in cloud connector) open for SaaS deployment in AppViewX.
- If the DNS validation is for HTTP challenge, it is essential to have port 80 accessible on the client machine to allow AppViewX to establish a connection.
- If the DNS validation is for DNS challenge, then the DNS server must be up and running and the DNS credentials file should be correctly configured.
- Certificate attributes and custom attributes must be configured to capture the attributes in the AppViewX GUI (if required).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

System Requirements

- **Operating System:** Windows Server 2019, Linux (Ubuntu 20, RHEL 8)
- **For IIS Server Binding:** Windows PowerShell 5.1 or later (Desktop edition) with .NET Framework 4.7.1 or later

Providing Sudo Permissions in Linux

1. To provide access to port 80 for a non-root user:
   a. Ensure that you are currently located within the POSHACME_AVX directory.
   b. Run the following command to grant the pwsh executable the capability to bind to port 80 without requiring root privileges:

      ```
      sudo setcap 'cap_net_bind_service=+ep' pwsh
      ```

      This step is essential to facilitate the http-01 challenge.
2. To add custom CA certificates to TrustStore:
   a. Determine the appropriate trust store on your Linux system. Common locations for trust stores are /etc/ssl/certs/ca-certificates.crt and /etc/ssl/certs/ca-bundle.crt.
   b. Obtain the acmetrustchain.crt file provided by the administrator from the POSHACME_AVX directory and place it in the trust-store of the machine.
   c. Log in as the root user. Run:

      ```
      sudo -i
      ```

   d. Copy the entire contents of the acmetrustchain.crt certificate chain file and append them to the end of the trust store file using the `cat` command:

      ```
      cat acmetrustchain.crt >> /etc/ssl/certs/ca-bundle.crt
      ```

   e. After execution, exit from the sudo user session.

Installing Posh-ACME

For Administrators

1. Download the latest version of Posh-ACME client from the AppViewX release portal.
2. Open your terminal/command prompt and navigate to the directory where the downloaded Posh-ACME ZIP file is present.
3. Unzip AppViewX_ACME_PoshACME_Client.zip to the current directory using the command:
   Linux

   ```
   unzip AppViewX_ACME_PoshACME_Client.zip
   ```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Windows

```
tar -xf AppViewX_ACME_PoshACME_Client.zip
```

4. Go to the extracted folder named POSHACME_AVX using the command:

```
cd POSHACME_AVX
```

5. Obtain server trust chain certificates. If the server certificate is created in AppViewX, download it from the AppViewX inventory, else download the certificate chain files (.pem or .crt) for the Certificate Authority (CA). This chain of files must include the root certificate as well as any intermediate certificates of the server.

   Linux

   If there are individual certificates for root CA and intermediate CAs, combine these certificate files into a single file. This can be done either through a text editor or by using the cat command:

```
cat intermediateca.crt rootca.crt > acmetrustchain.crt
```

   In this case, acmetrustchain.crt represents the name of the server trust chain certificate file. Now place this server trust chain certificate within the POSHACME_AVX directory.

   Windows

   If there are individual certificates for root CA and intermediate CA, then place the root CA certificates and intermediate CA certificates in the POSHACME_AVX directory under the RootCA and IntermediateCA folders, respectively.

6. Navigate from POSHACME_AVX to its parent directory using the command:

```
cd ..
```

7. Create a new zip archive named AppViewX_ACME_PoshACME_Client.zip for the POSHACME_AVX directory with the command:

   Linux

```
zip -r AppViewX_ACME_PoshACME_Client.zip POSHACME_AVX
```

   Windows

```
tar -a -c -f AppViewX_ACME_PoshACME_Client.zip POSHACME_AVX
```

   The resulting zipped folder can be shared among the users.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For Linux Users

1. Download the latest version of Posh-ACME client received from the administrator.
2. Open your terminal/command prompt and navigate into the directory where you downloaded the Posh-ACME ZIP file.
3. Unzip AppViewX_ACME_PoshACME_Client.zip using the command:

   ```
   unzip AppViewX_ACME_PoshACME_Client.zip
   ```

4. Go to the extracted folder named POSHACME_AVX using the command:

   ```
   cd POSHACME_AVX
   ```

5. Ensure the following permissions have been granted:
   - Port 80 access to a non-root user for HTTP challenge.
   - Presence of server trust chain certificates in the system truststore for SSL verification.

   Note: For more details, see Section, *Providing Sudo Permissions in Linux.*

6. Run:

   ```
   ./install.sh
   ```

   Running this command relocates the Powershell folder from the current directory to the current user's local/share/ directory.

7. Before performing CLM Actions, run:

   ```
   ./pwsh
   ```

   This command initiates the PowerShell environment. Ensure that you are in the POSHACME_AVX directory.

For Windows Users

1. Download the latest version of Posh-ACME client received from the administrator.
2. Open your command prompt as an administrator and navigate to the directory where you downloaded the Posh-ACME ZIP file.
3. Unzip AppViewX_ACME_PoshACME_Client.zip using the command:

   ```
   tar -xf AppViewX_ACME_PoshACME_Client.zip
   ```

4. Go to the extracted folder named POSHACME_AVX using the command:

   ```
   cd POSHACME_AVX
   ```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Ensure to add custom CA certificates to the TrustStore.
   In Windows, you can add the root CA and intermediate CA certificates located within the RootCA and Intermediate CA directories found in the POSHACME_AVX directory provided by the administrator to the *Trusted Root Certification Authorities* and *Intermediate Certification Authorities* stores, respectively.

   Access to these stores can be achieved through the **Manage Computer Certificates** control panel.
6. Run:

   ```
   install.bat
   ```

   Running this command relocates the Posh-ACME folder and Posh-ACME.Deploy folder from the current directory to the C:\Program Files\WindowsPowerShell\Modules\ directory.
7. Before performing CLM Actions, initiate Windows PowerShell environment as an administrator. Ensure you are in the POSHACME_AVX directory.

Actions using Posh-ACME

Enrolling Certificates

Prerequisites

1. Run the following command to import Posh-ACME:

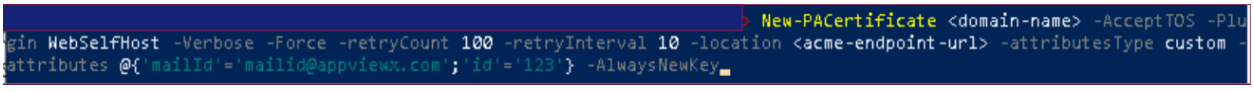
   ```
   Import-Module Posh-ACME -Force
   ```
2. Open PowerShell with admin privileges.
3. Ensure that you are in the POSHACME_AVX directory before you run the http-01 and dns-01 based challenge validation commands (described below) to enroll a certificate.

http-01 Based Challenge Validation

The command for an http-01 based challenge validation is:

```
New-PACertificate <Domain_Name> -AcceptTOS -Plugin WebSelfHost -Verbose -Force -retryCount <retryCount> -retryInterval <retryInterval> -location <ACME server endpoint URL> -attributes <Attributes> -attributesType <AttributesType> -AlwaysNewKey
```

A sample certificate enrollment command for HTTP validation is as shown:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

dns-01 Based Challenge Validation

Default DNS Challenge

The command for an dns-01 based challenge validation is:

```
New-PACertificate <Domain_Name> -AcceptTOS  -Contact <mail.id> -Plugin <Plugin_Name> -PluginArgs $pArgs -verbose -retryCount <retryCount>
-retryInterval <retryInterval> -location <ACME server endpoint URL> -attributes <Attributes> -attributesType <AttributesType> -AlwaysNewKey -Force
```

A sample certificate enrollment for DNS validation using route53 is as shown. Similarly other DNS plugins can be used.

Set-AWSCredential Command

```
Set-AWSCredential -StoreAs 'poshacme' -AccessKey '**********' -SecretKey '**********'
```

Purpose: This command stores AWS credentials under a named profile *poshacme*.

Parameters:

- -StoreAs 'poshacme': The name under which the AWS credentials are stored. This profile name is referenced later when configuring the Route 53 plugin.
- -AccessKey '**********': The AWS Access Key ID.
- -SecretKey '**********': The AWS Secret Access Key.

Plugin Arguments Configuration

```
$pArgs = @{R53ProfileName='poshacme'}
```

Purpose: This command sets up a hashtable $pArgs to store the Route 53 plugin arguments.

Key:

- R53ProfileName='poshacme': Specifies the AWS profile name (poshacme) to be used by the Route 53 plugin for authentication.

Enrollment Command

```
New-PACertificate <Domain_Name> -AcceptTOS -Plugin Route53 -PluginArgs $pArgs -attributesType cert -attributes @{'id'='0';'mail'='mailid@appviewx.com'} -retryCount 100 -retryInterval 12 -location <ACME server endpoint URL> -Verbose -Force -AlwaysNewKey
```

DNS Challenge

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
$pArgs==@{vendor='infoblox';vendorAccountName='infoblox'}
New-PACertificate <FQDN> -AcceptTOS -Contact <EMAIL> -Plugin Appviewx -PluginArgs $pArgs -retryInterval 30 -location <ACME_URL> -AlwaysNewKey
-Force -verbose
```

where the **vendor** value must be the DNS vendor name such as infoblox, **vendorAccountName** value must be the same as that configured in the AppViewX Integration Hub DNS Vendor settings, the **-Plugin** value must always be **Appviewx**.

Enterprise Secure Challenge

```
$pArgs=@{}
New-PACertificate <FQDN> -AcceptTOS -Contact <EMAIL> -Plugin Appviewx -PluginArgs $pArgs -retryInterval 30 -location <ACME_URL> -AlwaysNewKey
-Force -verbose
```

where the **pArgs** will be empty as there is no DNS vendor involved, the **Plugin** value must always be **Appviewx**.

Parameter Description

Parameters used in the http-01 and dns-01 based challenge validation

Parameter	Mandatory	Description
<ACME server endpoint URL>	Yes	Enter the appropriate ACME endpoint as configured in the AppViewX GUI.
<Domain_Name>	Yes	Enter a valid domain name for which the certificate needs to be enrolled. • Provide a **single domain name** to acquire a certificate for a particular domain. The domain name is the name of the order. Sample input for single domain name - *test1.appviewx.com* • Provide comma separated **multiple domain names** to acquire a certificate for all the given domains. The first domain name is the name of the order and is considered as the **main domain**, while the remaining domains are reflected in the Subject Alternative Names (SAN) of the certificate. Sample input for multiple domain names - *test2.appviewx.com,test3.appviewx.com*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters used in the http-01 and dns-01 based challenge validation (continued)

Parameter	Mandatory	Description
-attributes <Attributes> and **-attributesType <AttributesType>**	No	Posh-ACME can be run with **attributes**. These parameters allow you to provide multiple attributes. These attributes can include multiple name-value pairs, which are then included in the *Finalize Order* call along with the CSR. The values for these fields are provided as a JSON name/value pair, which can then be retrieved and mapped to the attributes in the application. This mapping enables you to include the attribute information in the certificate request for reporting purposes. For more information on the usage of attributes in Posh-ACME, see Defining Custom and Certificate Attributes.
-retryCount <retryCount> and **-retryInterval <retryInterval>**	No	These parameters allow you to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, see Polling during Enrollment/Renewal.
-Plugin <Plugin_Name>	Yes (only for dns-01 Based Challenge Validation)	Replace <Plugin_Name> with the appropriate powershell compatible DNS Plugin Name to perform DNS Validation. For more information on DNS plugins, see PoshACME DNS Plugins.
-PluginArgs $pArgs	Yes (only for dns-01 Based Challenge Validation)	Enter the appropriate plugin arguments for the chosen DNS plugin. For more information on the usage of DNS plugin arguments, see PoshACME DNS Plugins.

For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

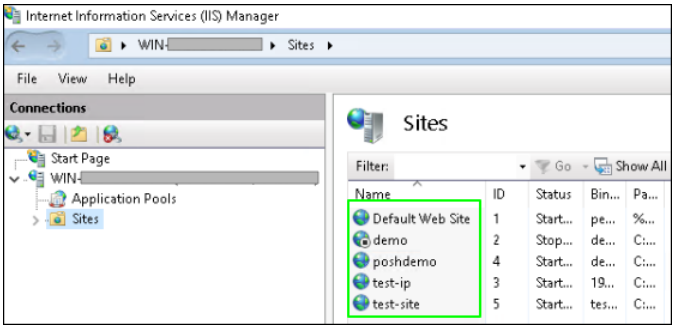
Binding Certificate to IIS Server in Windows

Posh-ACME supports issuance of certificates on their local IIS instance. To bind the certificate generated to local IIS instance, run:

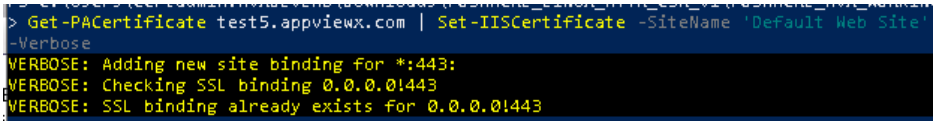
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
Get-PACertificate <Main_Domain_Name> | Set-IISCertificate -SiteName '<Site_Name>' -Verbose
```

Parameters used in the http-01 and dns-01 based challenge validation

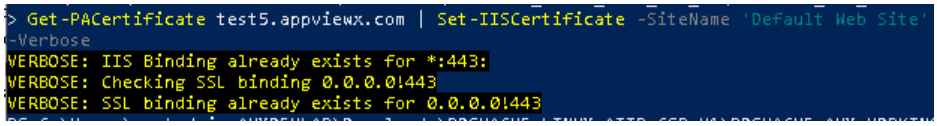
Parameter	Mandatory	Description
<Main_Domain_Name>	Yes	Enter a valid main domain name of the certificate to be bound.
<Site_Name>	Yes	Enter a valid IIS site name as shown: 

A sample command to bind a certificate to the IIS server is as shown:

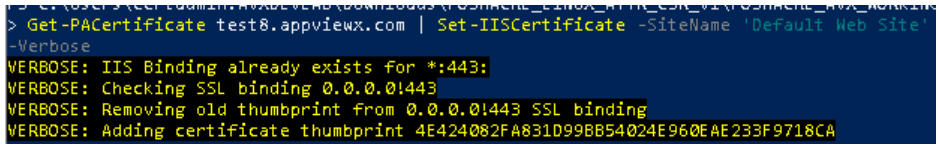


The certificate binding process only checks for the existence of an associated site binding.

- If a binding with the same domain name already exists, it will skip the binding process.



- If no such binding is found, it will proceed to bind the new certificate.



For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Working Behavior of Enrollment

Assuming there are multiple agents configured to the same server with distinct endpoint URLs, an example of the Agent X's Endpoint URL is `https://<server_hostname>:31443/avxapi/<acme_agent_x>/acme/directory`. Several scenarios can occur when enrolling a certificate for a domain name using ACME Agent X's Endpoint URL as described:

Scenario 1: No Previous Order Exists

If the domain-associated older order does not exist indicating that certificate enrollment for that domain has never been triggered:

- **Successful enrollment**: In the case of a successful enrollment, an order is created for that domain using Agent X's Endpoint URL and the certificate is successfully generated.
- **Interrupted/Failed enrollment**: If the enrollment process was interrupted or failed, an order may or may not be created for that domain using Agent X's Endpoint URL and the certificate is not generated.

Scenario 2: Previous Order Exists

If the domain-associated older order exists indicating that certificate enrollment for that domain was initiated earlier, this could be due to a previously successful enrollment or a previously interrupted enrollment call.

- **Successful enrollment**: If enrollment is successful, the previous domain-associated order linked to the domain is used, even if it was set up with a different Agent’s Endpoint URL. Attempting to use Agent X’s Endpoint URL will not work. The older certificate cannot be used and is backed up as a .bak file, while a new certificate is generated.
- **Interrupted/Failed enrollment**: If the enrollment process was interrupted or was unsuccessful, the domain-associated older order persists. The older certificate cannot be used and is backed up as a .bak file, and no new certificate is generated.

To address situations where the domain-associated older order’s Endpoint URL is being used instead of creating a new order with Agent X's Endpoint URL, a proposed solution is as follows:

1. Delete the domain-associated older order and associated certificate-related files. This allows for a new certificate issuance process using ACME Agent X’s Endpoint URL.
2. To delete the domain-associated older order, use the following command in the PowerShell environment:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
Remove PA-Order -Name <Domain_Name>
```

```
PS /home/appviewx/POSHACME_TEST/POSHACME_AVX> Remove-PAOrder -Name test4.appviewx.com

Deleting an order will also delete the certificate and key if they exist.
Are you sure you wish to delete order 'test4.appviewx.com'?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

Renewing Certificates

Certificates generated by POSH-ACME are renewed as needed. The system assesses the validity of all the certificates to identify those requiring renewal. This depends on the threshold specified during the execution of the renewal.ps1 script using the **renewalDaysThreshold** parameter. Certificates with a remaining validity period (measured in days) less than the specified threshold will only be considered for renewal.

Renewing Certificates

1. Open PowerShell with admin privilege.
2. Ensure that you are in the POSHACME_AVX directory before you run any commands to renew certificates.
3. Run:

```
./renewal.ps1 -retryCount <retryCount> -retryInterval <retryInterval> -renewalDaysThreshold <renewalDaysThreshold>
```

```
PS /home/appviewx/POSHACME_TEST/POSHACME_AVX> ./renewal.ps1 -retryCount 5 -retryIn
terval 4 -renewalDaysThreshold 20
```

The above command implies that certificates with a validity of less than 20 days are considered for renewal.

Parameters used in the renew command

Parameter	Mandatory	Description
-retryCount <retryCount> and **-retryInterval <retryInterval>**	No	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, see Polling during Enrollment/Renewal.
<renewalDaysThreshold>	No	Specify the threshold number of days. The default value is set to 30.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: When there is an incomplete renewal, the old certificate that is being renewed is deleted from the client's machine.

For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

Scheduling Tasks for Automated Certificate Renewal

Linux

A single scheduled task runs every day at a specified time and checks the validity of all the certificates to determine if any of them should be renewed based on the threshold **renewalDaysThreshold** specified.

To automate renewal for Posh-ACME through cron job, exit PowerShell environment and run:

```
(crontab -l ; echo "MM HH * * * <path to renewal.sh file> -retryCount <retryCount> -retryInterval <retryInterval> -renewalDaysThreshold <renewalDaysThreshold>
 -poshACMEDirectoryPath <poshACMEDirectoryPath> >> <path_to_renewal_log_file> 2>&1") | crontab -
```

Parameters used in the schedule task renew command (Linux)

Commands	Description
MM HH	Specify time for renewal in **HH** (hours), **MM** (minutes).
<path to renewal.sh file>	Specify the path to the renewal.sh file which is present in the POSHACME_AVX directory.
<poshACMEDirectoryPath>	Specify the path to the POSHACME_AVX folder.
<path_to_renewal_log_file>	Specify the path to a text file where automated renewal activities are logged. This file can be used to track renewal processes.
<renewalDaysThreshold>	Specify the threshold days renewal. The default value is set to 30.
-retryCount <retryCount> and **-retryInterval <retryInterval>**	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, see Polling during Enrollment/Renewal.

Example:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
[appviewx@i POSHACME_AVX]$ crontab -l
[appviewx@i POSHACME_AVX]$ (crontab -l ; echo "30 14 * * * /home/appviewx/nov_22
/posh/POSHACME_AVX/renewal.sh -retryCount 100 -retryInterval 10 -renewalDaysThre
shold 6000 -poshACMEDirectoryPath /home/appviewx/nov_22/posh/POSHACME_AVX/ >> /h
ome/appviewx/nov_22/posh/POSHACME_AVX/re.log 2>&1") | crontab -
[appviewx@i POSHACME_AVX]$ crontab -l
30 14 * * * /home/appviewx/nov_22/posh/POSHACME_AVX/renewal.sh -retryCount 100 -
retryInterval 10 -renewalDaysThreshold 6000 -poshACMEDirectoryPath /home/appview
x/nov_22/posh/POSHACME_AVX/ >> /home/appviewx/nov_22/posh/POSHACME_AVX/re.log 2>
&1
```

In the above example, the scheduled renewal task is triggered at 02:30 pm daily. Certificates that have less than 6000 days of remaining validity will qualify for renewal.

Note: See the renewalLogs.log file located in the POSHACME_AVX directory for logs of the certificate renewal process

Some helpful commands to use for the renewal process.

Parameters used in the schedule task renew command

Command	Description
date	Cron jobs operate according to the server's predefined timezone, typically set to UTC by default. You can verify this timezone by running the ***date*** command in the terminal. Scheduled tasks will commence in accordance with the cron system's understanding of time and time zones.
crontab -e	If you need to modify the time for a cron job that you have previously set up, you can adjust it by editing the time in the crontab file.
crontab -l	Used to check the scheduled cron jobs.

For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

A single scheduled task runs every day at a specified time and checks the validity of all the certificates to determine if any of them should be renewed based on the threshold **renewalDaysThreshold** specified.

To automate renewal for Posh-ACME through a scheduled task, open PowerShell with admin privilege (ensure that you are in the POSHACME_AVX directory) and run:

```
.\renewal_schedule_windows.ps1 -retryCount <retryCount> -retryInterval <retryInterval> -renewalDaysThreshold <renewalDaysThreshold> -time HH:MM
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters used in the schedule task renew command

Commands	Description
HH:MM	Specify time for renewal in **HH** (hours), **MM** (minutes).
<renewalDaysThreshold>	Specify the threshold days renewal. The default value is set to 30.
-retryCount <retryCount> and **-retryInterval <retryInterval>**	These parameters enable users to customize polling behavior by defining the number of retry attempts and the wait time between each attempt respectively. For more information on polling in Posh-ACME, see Polling during Enrollment/Renewal.

Example:

```
> .\renewal_schedule_windows.ps1 -retryCount 5 -retryInterval 2 -renewalDaysThres
hold 40 -time 14:30

Scheduled task named 'Posh-ACME Renewal' has been successfully created. It will r
un daily at 14:30 with a renewal days threshold of 40.
```

As per the above command, the scheduled renewal task is triggered at 02:30 pm on a daily basis. Certificates that have less than 40 days of remaining validity are subject to renewal.

For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

Working Behavior of Renewal

- **Successful Renewal:** When the renewal of a domain certificate is successfully completed, the older certificate cannot be used and is backed up as a .bak file and is then replaced with the newly generated certificate. This ensures that a copy of the older certificate is preserved while the updated certificate takes its place.
- **Interrupted Renewal:** If the renewal process is prematurely interrupted, the older certificates may not be successfully renewed. In such cases, the older certificates become unusable and they are deleted and backed up as a result of the interrupted renewal process.

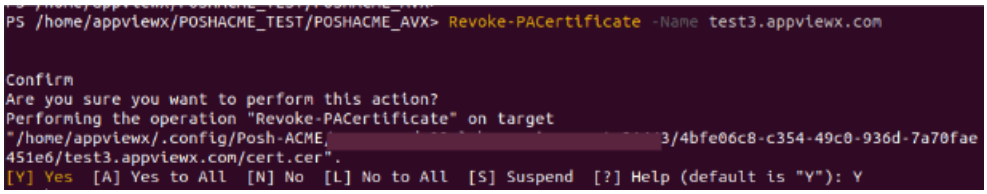
Revoking Certificates

Certificates can be revoked either by providing the certificate's **main domain** name or the **certificate file path**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

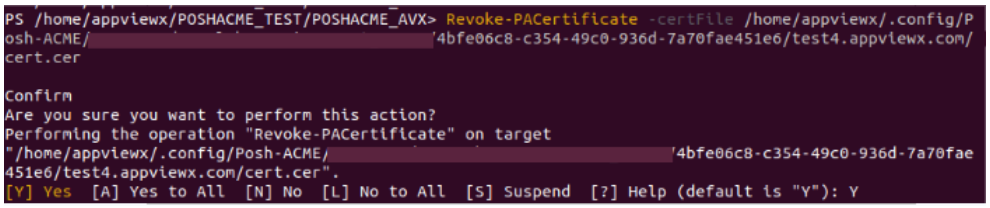
1. Open PowerShell with admin privileges.
2. Ensure that you are in the POSHACME_AVX directory before you run any commands to revoke certificates.
3. To revoke certificates:
   - By specifying the **main domain** name of the certificate.

```
Revoke-PACertificate -Name <Main_Domain_Name>
```



   - By specifying the **certificate file path**.

```
Revoke-PACertificate -certFile <certFilePath>
```



> **Tip:** To skip the revocation confirmation prompt, use the flag **-Force** along with the command.

Using the Revoke-PACertificate command does not automatically delete the order associated with the revoked certificate. Consequently, Posh-ACME makes renewal attempts for revoked certificates during the next scheduled renewal process. To avoid this, delete that specific domain-associated order manually.

For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

Executing Certbot with Enhanced Data

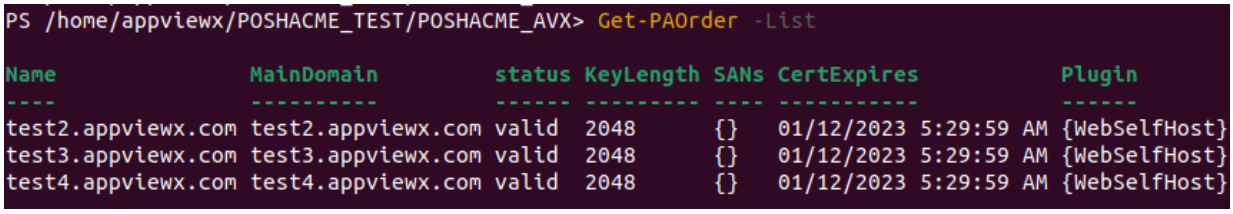
Accessing Orders and Certificates

The following set of commands are used for accessing orders and certificates:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- To return details such as domains, key length, expiration, and status for one or more ACME orders previously created, run:

```
Get-PAOrder -List
```



- To return details such as thumbprint, subject, validity, SANs, and file locations for one or more ACME certificates previously created, run:

```
Get-PACertificate -List | Format-List
```

- To return details such as Thumbprint, Subject, Validity, SANs, and file locations for a specific certificate, run:

```
Get-PACertificate <Main_Domain_Name> | Format-List
```

- The common OS specific certificate directory paths are as follows:
  - **Linux**: /home/<user>/.config/Posh-ACME/<server-name>/<account-id>/<order(Main_Domain_Name)>/
  - **Windows**: C:\Users\<user>\AppData\Local\Posh-ACME\<server-name>\<account-id>\<order(Main_Domain_Name)>\

  The files within this certificate directory must have the following contents:
  - cert.cer (Base64 encoded PEM certificate)
  - cert.key (Base64 encoded PEM private key)
  - cert.pfx (PKCS12 container with cert+key)
  - chain.cer (Base64 encoded PEM with the issuing CA chain)
  - chainX.cer (Base64 encoded PEM with alternate issuing CA chains)
  - fullchain.cer (Base64 encoded PEM with cert+chain)
  - fullchain.pfx (PKCS12 container with cert+key+chain)

Note: The password protecting the PFX files is **poshacme**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Defining Custom and Certificate Attributes

attributes and attribute-type

The **-attributes <Attributes>** parameter allows you to provide multiple attributes in the Posh-ACME command. To provide attributes, list each attribute in the format of **'attribute_name'='attribute_value'** and separate each attribute with a semicolon.

Sample input for **attributes**:

```
-attributes @{'id'='1098';'environment'='development';'Director'='director_id'}
```

The **-attributesType <AttributesType>** parameter must be accompanied with the **-attributes <Attributes>** parameter which takes in one of the following inputs **cert/custom/both**.

Sample input for **attributesType**:

```
-attributesType custom
```

Usage of attributes with attributesType

- When **attributesType** is passed as **cert**, the attributes from the **attributes** field are taken as certificate attributes.

  Sample certificate attributes input: `-attributes @{'Id'='1';'eai'='test';'inScope'='yes';'environment'='envi1'} -attributesType cert`

  The image shows the certificate attributes defined in the Posh-ACME command:

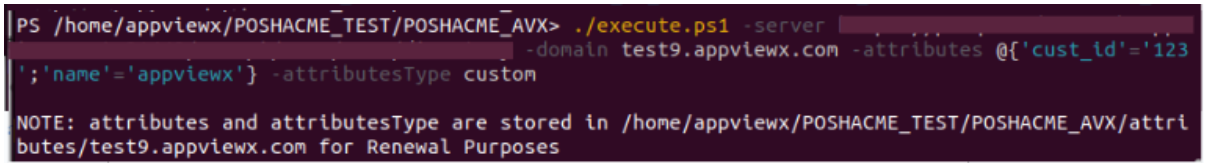
  The following image shows the certificate attributes and custom attributes sent as part of the request:

- When **attributesType** is passed as **custom**, the attributes from the **attributes** field are taken as custom attributes.

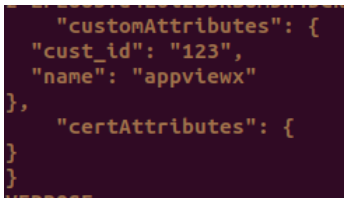
  Sample custom attributes input: `-attributes @{'cust_id'='123';'name'='appviewx'} -attributesType custom`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The image shows the certificate attributes defined in the Posh-ACME command:



The following image shows the certificate attributes and custom attributes sent as part of the request:



- When **attributesType** is passed as **both**, a JSON mapping is expected by the AppViewX Posh-ACME. A json file in the name attributesMapping.json needs to be created inside the POSHACME_AVX directory. There is a template file named attributesMappingTemplate.json present within the POSHACME_AVX directory, which can also be renamed to attributesMapping.json.

  A sample attributesMapping.json is as shown:

  ```
  {
  "senior_director" : "Sr Director",
  "intermediate_director" : "Intermediate Director"
  }
  ```

  - The *key* [in the *key:value* pair from attributesMapping.json] refers to the certificate attribute key provided in the command, while the *value* corresponds to the custom attribute key where the value of the certificate attribute must be passed.
  - The attributes passed as input are sent as certificate attributes and for the attributes present in the attributesMapping.json, the mapped value is being used as attribute name and sent as custom attribute.

  Sample certificate attributes input: `-attributes`

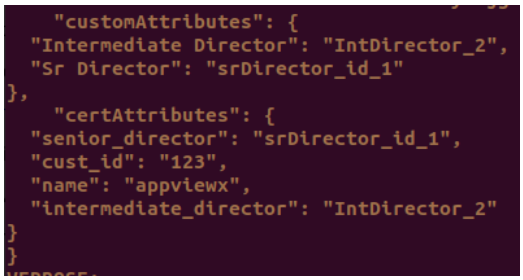
  `@{'cust_id'='123';'name'='appviewx';'senior_director':'srDirector_id_1','intermediate_director':'IntDirector_2'} -attributesType both`

  The image shows the attributes defined in the Posh-ACME command:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
PS /home/appviewx/POSHACME_TEST/POSHACME_AVX> ./execute.ps1 -server
                                              -domain test9.appviewx.com -attributes @{'cust_id'='123
';'name'='appviewx';'senior_director'='srDirector_id_1';'intermediate_director'='IntDirector_2'}
-attributesType both

NOTE: attributes and attributesType are stored in /home/appviewx/POSHACME_TEST/POSHACME_AVX/attri
butes/test9.appviewx.com for Renewal Purposes
```

The following image shows the certificate attributes and custom attributes sent as part of the request:



Some important points to note are:

- The use of *-attributes <Attributes> -attributesType <AttributesType>* is optional.
- Omitting this parameter will not disrupt the current flow of certificate creation. You may proceed with the certificate generation process without any issues.
- The values provided in the **attributes** field and **attributesType** field while enrolling are stored in a folder named attributes inside the POSHACME_AVX directory under the name of the certificate's domain.
- These values are fetched and used when the certificate of that domain name is being renewed.

Polling during Enrollment/Renewal

Polling can be activated when manual approval is configured for certificate generation. In this scenario, the client conducts polling for the certificate within a specified timeframe as determined by the configured parameters. If the certificate is approved before the polling duration expires, it will be retrieved. To enable polling in the certbot client, you can pass the following parameters as mentioned:

Parameters to be passed with Posh-ACME commands

Parameters	Type	Mandatory	Description
-retryInterval	Integer	No	The waiting period (in seconds) after which the next call in the polling is triggered. [Default value : 2]
-retryCount	Integer	No	The number of times the certificate is polled from the client side.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters to be passed with Posh-ACME commands (continued)

Parameters	Type	Mandatory	Description
			[Default value : 30]

A sample usage of the above parameters: `-retryCount 8 -retryInterval 5`

In this example, the **-retryInterval** is set to 5 seconds, and the **-retryCount** is set to 8. Hence, the certificate will be polled 8 times (retryCount) with a 5 second interval (retryInterval) for each polling attempt. The polling process will take a total of 8 * 5 = 40 seconds to complete.

Points to note:

- The use of *-retryCount <retryCount>* and *-retryInterval <retryInterval>* is optional and is required only when the **Certificate Requests Need Approval** attribute is enabled in the CA policy settings of the ACME Server.
- Omitting these parameters will not disrupt the current flow of certificate creation.
- If necessary, the default values for polling are used. You may proceed with the certificate generation process without any issues.

Providing CSR and EAB Fields

Fields to be provided in the CSR and for External Account Binding (EAB) can be configured in a JSON file. A JSON file in the name certConfig.json with the configured fields needs to be created inside the POSHACME_AVX directory. There is a template file named certConfigTemplate.json present within the POSHACME_AVX directory, which can be renamed to certConfig.json.

CSR fields that can be provided:

- Subject fields:
  - Organization
  - Organization unit
  - Country
  - State
  - Locality
- Hashing algorithm (when using RSA)
- Key-Size

EAB fields that can be provided:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- EAB hmac
- EAB kid
- EAB Algorithm

A sample certConfig.json is as shown:

```
{
"csr_params": {
        "organization" : "cert_appviewx",
        "organization_unit" : "crypto_avx",
        "country" : "IN",
        "state" : "Andhra Pradesh",
        "locality" : "Rajahmundry",
        "hashing_algorithm":"SHA384",
        "key_size":"2048"
        },
"eab": {
        "kid":"",
        "mac":"",
        "alg":"hs256"
}
}
```

Note:

- When EAB is not configured on the server side, the fields for *kid*, *mac*, and *alg* can be configured to empty strings ("").
- If you intend using the default configuration of Posh-ACME, you may set the fields in the certConfig.json file to empty strings ("").

For more information on the keywords used in the Posh-ACME commands, see Keywords in Posh-ACME commands.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Best Practices

- **Prefer Stronger Key Sizes:** Use higher key sizes where applicable—consider using RSA 2048 or above for increased cryptographic strength.
- **Distribute Renewal Schedules:** Ensure that certificate renewal cron jobs or schedulers are spread out in time to avoid concentrated load on the ACME server and ensure smooth, uninterrupted renewals.
- **Use External Account Binding (EAB):** Use EAB as an added layer of authentication for enhanced security.
- **Secure your API credentials:** Store DNS provider API keys securely (e.g., environment variables, encrypted files).
- **Challenge methods:** Customize plugins with fallback and retries if DNS propagation is slow.
- **Automation:** Use scheduled tasks or pipelines (like Jenkins/GitHub Actions) to automate renewals. Use **Renew-PAOrder** in a loop or job script.
- **Deployment**: Use **Export-PACertificate** with **-OutPath** or **-PfxPass** for downstream systems.
- **Automate deployment to**:
  - **IIS**: Import-PfxCertificate, New-WebBinding
  - **Remote systems**: use PowerShell Remoting, WinRM, or secure file copy.
- **Secure Storage**: Avoid storing API keys in plain text. Use PowerShell's **ConvertTo-SecureString** and **Export-Clixml**.
- **Custom Package Verification**: Make sure the AppViewX DNS plugin is available in Posh-ACME package if the user is using the AppViewX DNS Challenge or the Enterprise Secure DNS Challenge option.

Troubleshooting

Accessing ACME Logs

1. Access the terminal window.
2. Go to <Installed_Path>/logs directory and find the name format with <avxgw-HTTPS-<yyyy-mm-dd>.log>, for example, <avxgw-HTTPS-2021-03-17.log>
   - If the file size exceeds 100MB, it will be rolled over and the latest logs will be available in the latest file named with an incrementing counter starting from 1 such as avxgw-HTTPS-<yyyy-mm-dd>.<incrementing_counter>.log, for example, <avxgw-HTTPS- 2021-03-17.1.log>.
   - ACME plugin logs:

     </home/appviewx/appviewx/logs/avx-vendor-cert-acme-agent-<pod_name>.log>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General Errors

General errors that can be encountered

1. Invalid End-point URL	
Description	When an invalid ACME endpoint URL is provided in Posh-ACME, it will result in the following error.
Error	`Set-PAServer: Name or service not known`
Troubleshooting	Ensure that the provided URL is valid and set up through the AppViewX GUI.
2. CA Certificate not configured in the client's trust store	
Description	When the CA certificate of the ACME server is not configured in the client's trust store, the following error is expected.

Error	`Set-PAServer: The remote certificate is invalid because of errors in the certificate chain: PartialChain`
	
	or
	
	`Set-PAServer: The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.`

Troubleshooting	See Point 2 (To add custom CA certificates to TrustStore) in the Section, Providing Sudo Permissions in Linux.
3. Invalid Acme Agent	
Description	When the specified ACME agent name in the endpoint URL does not match any configured agent in the AppViewX GUI, it will trigger the following error.
Error	`Set-PAServer: {"detail":"Unable to fetch acme server url. - Agent Settings name given is invalid","type":"urn:ietf:params:acme:error:serverInternal"}`
Troubleshooting	Ensure that the provided URL is valid and set up through the AppViewX GUI.
4. Invalid Port in the End-point URL	
Description	This error is expected when invalid port details are provided in the acme end-point URL.

Error	`InvalidArgument: /home/<user>/.local/share/powershell/Modules/Posh-ACME/4.18.0/Public/Set-PAServer.ps1:53`
	`Line |`
	`53 | $uri = [uri]$DirectoryUrl`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General errors that can be encountered (continued)

		~~ | Cannot convert value "https://<server_hostname>:31443234/avxapi/<acme_agent>/acme/directory" to type "System.Uri". | Error: "Invalid URI: Invalid port specified."
Troubleshooting	Ensure that the port specified in the URL is valid.
5. Port 80 permission is missing for PowerShell	
Description	When PowerShell pwsh executable lacks the capability to bind to port 80 without requiring root privileges, it will result in the following error.

Error	`MethodInvocationException: Exception calling "Start" with "0" argument(s): "Permission denied"`
	or
	`Exception calling "Start" with "0" argument(s): "Access is denied"`

Troubleshooting	See Point 1 (To provide access to port 80 for a non-root user) in the Section, Providing Sudo Permissions in Linux.
6. Invalid Domain Name	
Description	When an enrollment call is made for an invalid domain name, the certificate issuance process will not proceed.
Error	Exception: /home/<user>.local/share/powershell/Modules/Posh-ACME/4.18.0/Public/New-PACertificate.ps1:271 Line | 271 | Submit-ChallengeValidation | ~~~~~~~~~~~~~~~~~~~~~~~~~~ | Authorization invalid for example.appviewx.com:
Troubleshooting	In order for the domain to be considered valid and for the certificate issuance to succeed, a proper DNS entry must be made for the server corresponding to the domain before attempting to enroll a certificate for it.
7. Incorrect usage of attributes and attributesType fields	
Description	When only one field - either the ‘attributes’ or ‘attributesType’ is provided in the arguments of the enrollment command, it results in the following error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General errors that can be encountered (continued)

Error	Submit-OrderFinalize: Attribute type must be one of the following values : cert/custom/both) Both attributes and attributesType must be provided to add attributes in the certificate request...
Troubleshooting	The **attributesType** field must be accompanied with the **attributes** field. See Accessing Orders and Certificates section for more information.
8. Incorrect attributeType	
Description	An incorrect value is provided for the **-attributesType** field.
Error	Submit-OrderFinalize: Attribute type must be one of the following values : cert/custom/both)
Troubleshooting	The **attributesType** field must be one of the following values : cert/custom/both). See the Accessing Orders and Certificates section for more information.
9. Incorrect IIS Site Name	
Description	An incorrect IIS site name is used for the field -SiteName.
Error	Set-IISCertificate : Site <Site_Name> not found.
Troubleshooting	The 'SiteName' field must be valid (present in the Sites of IIS Manager of the machine).
10. Missing EAB Credentials	
Description	EAB Credentials ('eab:hmac' and 'eab:key' fields) are set to empty string ("") in the 'certConfig.json' file, while the end-point server requires external account credentials.
Error	New-PACertificate : The current ACME server requires external account credentials to create a new ACME account. Please run New-PAAccount with the ExtAcctKID and ExtAcctHMACKey
Troubleshooting	Provide valid EAB credentials for the 'eab:hmac' and 'eab:key' fields in the 'certConfig.json' file.
11. Invalid EAB Kid	
Description	Incorrect EAB kid is provided in the 'certConfig.json' file.
Error	New-PACertificate: The "externalAccountBinding.protected" field is invalid.:: kid is invalid
Troubleshooting	Provide a valid EAB kid which is configured in AppViewX ACME configuration settings.
12. Invalid EAB Algorithm	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

General errors that can be encountered (continued)

Description	Incorrect EAB Algorithm is provided in the ‘certConfig.json’ file.
Error	New-PACertificate : Some of the errors was found in request.
Troubleshooting	Provide a valid EAB Algorithm which is configured in AppViewX ACME configuration settings.
13. Invalid Key Length	
Description	Incorrect key length is provided in the ‘certConfig.json’ file.
Error	New-PACertificate : Cannot validate argument on parameter 'CertKeyLength'. Must be 'ec-256','ec-384','ec-521' for EC keys or between 2048-4096 (divisible by 128) for RSA keys
Troubleshooting	Provide valid key length value. Must be 'ec-256','ec-384','ec-521' for EC keys or between 2048-4096 (divisible by 128) for RSA keys.

#	Error Message	Description	Troubleshooting
1	Self DNS Challenge token validation/IP Validation option is selected but EAB details/Allowed domains are not configured for the agent settings.	When AppViewX **DNS Challenge** or **Enterprise Secure Challenge Validations** is selected but **Allowed Domains** or EAB details are not provided from the ACME client, you get this error.	1. Provide valid domains under the **Allowed Domains** field. 2. Enable either **Static EAB** or **Dynamic EAB credentials**.
2	DNS Challenge validation failed. IP Options are not selected for agent settings. Allowed options are STRICT, ANY, NONE.	If Enterprise Secure Challenge type other than **Secure, Any, Ignore** is selected in the ACME Settings.	Select any one of the following under Enterprise Secure Challenge options: **Secure, Any, Ignore.**
3	DNS Challenge validation failed. ACME DNS challenge verification via DNS A record failed. For STRICT Option IP didn't Match.	If the **Secure** option is selected under **Enterprise Secure Challenge** type and the ACME client’s IP address does not match	Make sure that the DNS A record of the requesting domain contains the same IP address as the ACME client's IP address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
		with the available DNS A record for the particular domain.	
4	DNS Challenge validation failed. ACME DNS challenge verification via DNS A record failed. For STRICT Option there are more IP address entries in DNS A Record.	If the **Secure** option is selected under **Enterprise Secure Challenge** type and the DNS A record for the requesting domain is fetched with more than one IP address.	Make sure that the DNS A record of the requesting domain contains only one IP address, which is the same as the ACME client's IP address.
5	DNS Challenge validation failed. No DNS A records are found to validate ANY type.	If the **ANY**option is selected under **Enterprise Secure Challenge** type and the DNS A records for the requesting domain are fetched in which none of the IP address matches with the ACME client’s IP address.	Make sure that the DNSA records of the requesting domain contains any one IP address, which is the same as the ACME client’s IP address.
6	DNS Challenge validation failed. DNS A record for the domain <domain name> is not available.	When AppViewX is not able to obtain the DNS A records for the requesting domain.	• Check if the DNS Server is reachable from AppViewX to resolve and obtain the DNS A records of the requesting domain. • Check if the provided DNS server hostname is proper to resolve and obtain the DNS A records.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
7	DNS Challenge validation failed. Error while executing Create/Delete record operation.	1. When AppViewX is not able to reach the DNS server for creating DNS TXT for the requesting domain. 2. When there are errors while performing creation or deletion of DNS TXT records in the DNS server.	1. Check if the DNS server is reachable from AppViewX. 2. Check AppViewX logs for detailed errors regarding creation and deletion of errors.

Keywords in Posh-ACME commands

Keywords used in the Posh-ACME commands

Keyword	Expected Input	Comments
-domain	<Domain_Name> (Type: String) **domain1.com** (or) **domain1.com, domain2.com, domain3.com**	Comma-separated list of domains to obtain a certificate for.
-server	<Acme Server Endpoint URL fetched from AppViewX GUI> (Type: String)	ACME Directory Resource URI.
-attributes	[format: @{'id'='1098';'environment'='development';'Director'=' director_id'}]	The -attributes field allows users to provide multiple attributes in the format of **'attribute_name'='attribute_value'** and separate each attribute with a semicolon in the Posh-ACME command.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Keywords used in the Posh-ACME commands (continued)

Keyword	Expected Input	Comments
		[optional, but **-attributes** field must be accompanied with the **-attributesType** field]
-attributesType	Any one of the following : **cert/ custom/both** (Type: String)	Takes in one of the following inputs **cert/custom/both**. [optional, but must be included when **-attributes** is passed]
-retryInterval	<retryInterval> (Type: Integer)	The waiting period in seconds, after which the next call in the polling is triggered. [Default value : 2] (Optional)
-retryCount	<retryCount> (Type: Integer)	The number of times for which the certificate is polled from the client side. [Default value : 30] (Optional)
-renewalDaysThreshold	<renewalDaysThreshold> (Integer)	Threshold value for renewal. Certificates with a remaining validity period (measured in days) less than the specified threshold will only be considered for renewal. [Default value: 30] (Optional)
-poshACMEDirectoryPath	<poshACMEDirectoryPath>	Path to the POSHACME_AVX folder.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Keywords used in the Posh-ACME commands (continued)

Keyword	Expected Input	Comments
-Name	<Main_Domain_Name> (Type: String)	The main domain name of the certificate. It is the same as the order name.
-SiteName	<Site_Name> (Type: String)	Name of the site in IIS.
-certFile	<certFile> (Type: String)	Path to the certificate to be revoked.

Keywords in Posh-ACME certConfig.json

Json keys used in the Posh-ACME certConfig.json file

Json keys	Type	Comments
csr_params:organization **csr_params:organization_unit** **csr_params:country** **csr_params:state** **csr_params:Locality**	String	Choose the appropriate subject fields for the CSR. (Optional)
csr_params:hashing_algorithm	String	Hashing algorithm for signing (RSA). Specify any one algorithm from {SHA256, SHA384, SHA512}. [Default value: SHA384] (Optional)
csr_params:key_size	String	The type and size of private key to use for the certificate. For RSA keys, specify a number between 2048-4096 (divisible by 128). For ECC keys, specify either 'ec-256'\'ec-384'\'ec-521'.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Json keys used in the Posh-ACME certConfig.json file (continued)

Json keys	Type	Comments
		[Default value: 2048] (Optional) Whenever ECC keys are used, the hashing algorithm is set internally and cannot be changed from configuration file.
eab:kid	String	The value of Key Identifier for External Account Binding. (Optional)
eab:hmac	String	The value of HMAC key for External Account Binding. (Optional)
eab:alg	String	Signature Algorithm for External Account Binding. Specify any one algorithm from {HS256, HS384, HS521}. [Default value: HS256] (Optional)

Configuring AppViewX LEGO Client

AppViewX introduces LEGO client--an ACME client similar to the AppViewX EST client. This client incorporates major customizations implemented in all ACME clients provided by AppViewX, including Posh-ACME, win-acme, and Certbot.

This section explains implementation of LEGO client for Microsoft Windows and Linux.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

- LEGO client has no installation steps. The binary will be provided for both Microsoft Windows and Linux and can be consumed directly.
- For Windows, use the administrator command prompt for all the commands.
- For Linux:
  - **DNS:** Does not require sudo.
  - **HTTP:** This first command alone will require sudo.

```
sudo setcap 'cap_net_bind_service=+ep' <legoClient-binary>
```

- EAB is mandatory for LEGO plug-in.
- --dns.propagation-disable-ans flag is mandatory for enrollment and renewal as self-challenge validation must be disabled in these cases.
- Revocation command is similar to others.
- DNS challenge details
  1. --vendor -> vendor name [currently only infoblox is supported]
  2. --vendor-account -> vendor account name -> name of the configuration in integration hub
  3. Integration hub must be configured with the DNS server details.

```
Command:
./legoClient --domains <Domain-name-comma-seperated> --email <Email-id> --dns appviewx --accept-tos=true --server=<ACME-Directory-URL>
 --tls-skip-verify  --eab --kid "<KID>" --hmac "<HMAC>" --eab-algorithm <EAB-Algorithm> --dns.propagation-disable-ans --vendor <Vendor-name>
 --vendor-account <Vendor-Account-Name> run
```

- Enterprise secure challenge:

```
Command:
./legoClient --domains <Domain-name-comma-seperated> --email <Email-id> --dns appviewx --accept-tos=true --server=<ACME-Directory-URL>
 --tls-skip-verify  --eab --kid "<KID>" --hmac "<HMAC>" --eab-algorithm <EAB-Algorithm> --dns.propagation-disable-ans run
```

Windows Commands

Component/ Function	Command
Enroll HTTP	legoClient.exe --email= example@email.com --domains=domain.example.com --server=https://server.example.com:port/api/lego_http/acme/directory --http --tls-skip-verify run

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Component/ Function	Command
Enroll EAB HTTP	legoClient.exe --email=example@email.com --domains=domain.example.com --server=https://server.example.com:port/api/lego_http/acme/directory --http --tls-skip-verify --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS512 run
DNS enroll (AWS Route 53)	set AWS_PROPAGATION_TIMEOUT=40 set AWS_ACCESS_KEY_ID=<aws-access-key-id> set AWS_SECRET_ACCESS_KEY=<aws-secret-access-key> set AWS_REGION=<aws-region> legoClient.exe --domains <domain> --email example@email.com --dns <dns-provider> --accept-tos=true --organization-name <organization-name> --organizational-unit <organizational-unit> --country <country-code> --province <province> --server https://<server>:<port>/avxapi/lego_dns/acme/directory --tls-skip-verify run **Note:** DNS configurations can vary depending on the DNS providers. For more information, refer to https://go-acme.github.io/lego/dns/.
DNS enroll (AppViewX)	legoClient.exe --domains <DOMAIN-NAMES> --email <EMAIL> --dns appviewx --accept-tos=true --server=<ACME-SERVER-URL> --tls-skip-verify --eab --kid "<EAB-KID>" --hmac "<EAB-HMAC>" --eab-algorithm <EAB Algorithm> --dns.propagation-disable-ans --vendor <dns-vendor-name> --vendor-account <vendor-account-name> run
Sample for custom and cert attributes	legoClient.exe --email=example@email.com --domains=domain.example.com --server=https://server.example.com:port/ api/lego_http/acme/directory --http --tls-skip-verify --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS512 --cert-emails "email1@example.com,email2@example.com" --province <province> --country <country-code> --organizational-unit <organizational-unit> --organization-name <organization-name> --cert-attributes "<cert-attributes>" --custom-attributes "<custom-attributes>" run **Sample for Customer and Certificate Attributes in case of multiple values:** --cert-attributes "aa=apple,bb=ball" --custom-attributes "test=customattribute1,test2=customattribute2"

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Component/ Function	Command
Renew all	legoClient.exe --tls-skip-verify renew --renew-all --days <number-of-days> --no-random-sleep **Note:** --days indicates that the certificates will be renewed if their remaining validity is less than the number of days specified.
Renew one	legoClient.exe --email=example@email.com --domains=domain.example.com --server=https://server.example.com:port/api/lego_http/acme/directory --http --tls-skip-verify --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS512 --cert-attributes <cert-attributes> --custom-attributes <custom-attributes> renew --days <number-of-days>
DNS renew (AppViewX)	legoClient.exe --domains <DOMAIN-NAMES> --email <EMAIL> --dns appviewx --accept-tos=true --server=<ACME-SERVER-URL> --tls-skip-verify --eab --kid "<EAB-KID>" --hmac "<EAB-HMAC>" --eab-algorithm <EAB Algorithm> --dns.propagation-disable-ans --vendor <dns-vendor-name> --vendor-account <vendor-account-name> renew
Revoke	legoClient.exe --email=example@email.com --domains=domain.example.com --server=https://server.example.com:port/ api/lego_http/acme/directory --http --tls-skip-verify revoke <revocation reason>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Component/ Function	Command
	Note: Revocation reasons can include any of the following: • unspecified (0) • keyCompromise (1) • cACompromise (2) • affiliationChanged (3) • superseded (4) • cessationOfOperation (5) • certificateHold (6) • removeFromCRL (8) • privilegeWithdrawn (9) • aACompromise (10)
Reinstate	legoClient.exe --email=example@email.com --domains=domain.example.com --server=https://server.example.com:port/api/lego_http/acme/directory --http --tls-skip-verify revoke 8 **Note:** It is important to include the `--keep` flag at the end of the reinstate command; else, the certificates will be deleted after the operation.
Windows schedule command	legoClient.exe --tls-skip-verify renew --renew-all --days <number-of-days> --no-random-sleep --schedule "HH:MM" --schedule-only

Linux Commands

Component/ Function	Command
Enroll HTTP	./legoClient --domains <domain> --email example@email.com --accept-tos=true --server https://<server>:<port>/api/lego_http/acme/directory --tls-skip-verify --http run

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Component/ Function	Command
Enroll EAB HTTP	./legoClientLinux --domains <domain> --email example@email.com --accept-tos=true --server https://<server>:<port>/api/lego_http/acme/directory --tls-skip-verify --http --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS512 run
DNS enroll (AWS Route 53)	AWS_PROPAGATION_TIMEOUT=40 AWS_ACCESS_KEY_ID=<aws-access-key-id> AWS_SECRET_ACCESS_KEY=<aws-secret-access-key> AWS_REGION=<aws-region> ./legoClientLinux --domains <domain> --email example@email.com --dns <your-dns-provider> --accept-tos=true --server https://<server>:<port>/api/lego_dns/acme/directory --tls-skip-verify run **Note:** DNS configurations can vary depending on the DNS providers. For more information, refer to https://go-acme.github.io/lego/dns/.
DNS enroll (AppViewX)	./legoClient --domains <DOMAIN-NAMES> --email <EMAIL> --dns appviewx --accept-tos=true --server=<ACME-SERVER-URL> --tls-skip-verify --eab --kid "<EAB-KID>" --hmac "<EAB-HMAC>" --eab-algorithm <EAB Algorithm> --dns.propagation-disable-ans --vendor <dns-vendor-name> --vendor-account <vendor-account-name> run
Custom and cert attributes	./legoClientLinux --domains <domain> --email example@email.com --accept-tos=true --server https://<server>:<port>/api/lego_http/acme/directory --tls-skip-verify --http --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS384 --cert-attributes '<cert-attributes>' --custom-attributes '<custom-attributes>' run **Sample for Customer and Certificate Attributes in case of multiple values:** --cert-attributes 'aa=apple,bb=ball' --custom-attributes 'test=customattribute1,test2=customattribute2'
Renew all	./legoClientLinux --renew-all --tls-skip-verify renew --days <number-of-days> --no-random-sleep

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Component/ Function	Command
	Note: --days indicates that the certificates will be renewed if their remaining validity is less than the number of days specified.
Renew one	./legoClientLinux --domains <domain> --email example@email.com --accept-tos=true --server https://<server>:<port>/api/lego_http/acme/directory --tls-skip-verify --http --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS384 --cert-attributes '<cert-attributes' --custom-attributes '<custom-attributes>' renew --days 368
DNS renew (AppViewX)	./legoClient --domains <DOMAIN-NAMES> --email <EMAIL> --dns appviewx --accept-tos=true --server=<ACME-SERVER-URL> --tls-skip-verify --eab --kid "<EAB-KID>" --hmac "<EAB-HMAC>" --eab-algorithm <EAB Algorithm> --dns.propagation-disable-ans --vendor <dns-vendor-name> --vendor-account <vendor-account-name> renew
Revoke	./legoClientLinux --domains <domain> --email example@email.com --accept-tos=true --server https://<server>:<port>/api/lego_http/acme/directory --tls-skip-verify --http --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS384 --cert-attributes '<cert-attributes>' --custom-attributes '<custom-attributes>' revoke <revocation reason code> **Note:** Revocation reasons can include any of the following: • unspecified (0) • keyCompromise (1) • cACompromise (2) • affiliationChanged (3) • superseded (4) • cessationOfOperation (5) • certificateHold (6) • removeFromCRL (8) • privilegeWithdrawn (9) • aACompromise (10)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Component/ Function	Command
Suspend	./legoClientLinux --domains <domain> --email example@email.com --accept-tos=true --server https://<server>:<port>/api/lego_http/acme/directory --tls-skip-verify --http --eab --kid <EAB-KID> --hmac <EAB-HMAC> --eab-algorithm HS384 --cert-attributes '<cert-attributes>' --custom-attributes '<custom-attributes>' revoke 6 **Note:** It is important to include the `--keep` flag at the end of the suspend command; else, the certificates will be deleted after the operation.
Linux cron scheduler	legoClient --tls-skip-verify renew --renew-all --days <number-of-days> --no-random-sleep --schedule "MM HH * * *" --schedule-only

Troubleshooting

Windows acme client > HTTP challenge (especially for IIS)

If the **IIS challenge validation** fails (when using the **IIS webroot** method), even though the hostname correctly resolves to the Windows server and the required ports are open, verify the **MIME types** configuration for the IIS site. Click **Add** under **MIME Types**, and add the following entries:

- **File name extension:** `.`
- **MIME type:** `application/json`

SCEP

What is SCEP?

Simple Certificate Enrollment Protocol (SCEP) is an open source certificate management protocol to enable easier, scalable and secure certificate issuance. The primary characteristics of SCEP are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The request/response model is based on HTTP and supports RSA-based cryptography.
- Requires the use of a *challenge password* within the certificate signing request (CSR) which is shared between the server and the requester.
- Does not support certificate revocation online, and has limited Certificate Revocation List (CRL) retrieval support.

Note: AppViewX does not inherently rely on Network Device Enrollment Service (NDES); instead, it uses its own built-in server for the SCEP protocol. This gives AppViewX the advantage of seamlessly integrating with any Certificate Authority, unlike NDES, which is primarily tied to Microsoft Active Directory Certificate Services (ADCS).

How does SCEP work?

- **Gateway API URL:** SCEP allows devices to communicate with PKI through API URL, and then the users can put this URL in the mobile device management (MDM) for sending a payload to devices for which the client certificates are to be enrolled.
- **Shared Secret:** A shared secret is a case-sensitive challenge password shared between the SCEP server and the certificate authority (CA) to verify the CA with the appropriate server for signing certificates.
- **Certificate Request:** After the SCEP gateway is set and the shared secret is exchanged between the server and the CA, a configuration profile is developed to allow auto-enrollment of certificates for managed devices. Once the CA authenticates, the signed certificate is deployed on the device.
- **Signing Certificate:** The MDMs require SCEP signing certificate which is signed by the CA and includes the entire certificate chain of trust (Root CA, Intermediate CA and the signing certificate).

The SCEP enrollment and usage generally follows this workflow:

1. Obtain and validate a copy of CA certificate.
2. Generate CSR and send it to CA.
3. Poll the SCEP server to verify whether the certificate is signed.
4. Re-enroll for obtaining new certificates before the existing certificate expires.
5. Retrieve the CRL as needed, the preferred method is via a CRL distribution point (CDP) query.

Why is SCEP used?

Issuing public key infrastructure certificates requires an extensive process of information exchange and approval procedures with a trusted certificate issuing entity or certificate authority (CA). SCEP helps in automating the entire process, thus making it simpler, easier and faster for the IT security teams to

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

enroll and deploy certificates onto devices without any manual process. A device can easily enroll for certificates by using URL and a shared secret to communicate with CA. Mobile Device Management (MDM) systems like Microsoft Intune and Apple use SCEP for enrolling PKI certificates for the increasing number of smartphones and mobile devices.

The SCEP protocol services can be configured in AppViewX to enable the communications between the client (device endpoints) and AppViewX northbound services that processes the client requests such as certificate enrollment and renewal. Once the protocol service gets enabled, AppViewX will act as an RA in receiving and serving the client requests. The protocol must be enabled as an HTTP service.

What's Next?

- Configuring AppViewX SCEP Server

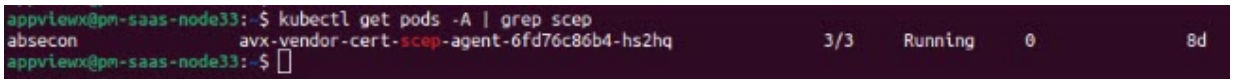
Configuring AppViewX SCEP Server

Prerequisites

Onprem

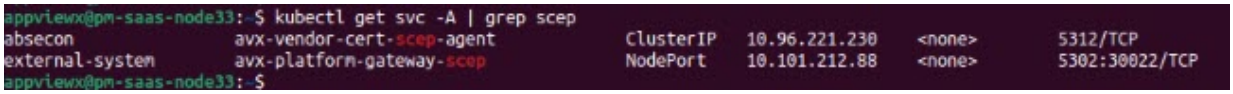
- Make sure that the SCEP pod is running in the cluster by using the command:

```
kubectl get pods -A | grep scep
```



- Make sure that <avx-platform-gateway-scep> and <avx-vendor-cert-scep-agent> services are running in the cluster by running:

```
kubectl get svc -A | grep scep
```



SaaS

Ensure the https gateway is enabled on the cloud connector while installing it. To do this:

1. Navigate to the installation directory of the cloud connector software.
2. Run

```
cd deps/tools
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Run

```
./k3s kubectl get svc -A | grep http
```

Note: It should have the avx-mid-server-gateway-http or avx-mid-server-gateway-https under namespace cc.

```
[appviewx@pe-qa-cc-n8 tools]$ ./k3s kubectl get svc -A | grep http
cc            avx-mid-server-gateway-http     NodePort    10.43.0.23     <none>        5302:30022/TCP
cc            avx-mid-server-gateway-https    NodePort    10.43.0.197    <none>        5300:30020/TCP
[appviewx@pe-qa-cc-n8 tools]$
```

Enabling SCEP Services

For Onprem

1. Log onto the AppViewX installer node. Open the terminal window.
2. Go to </installation_folder/appviewx_kubernetes/scripts> folder.
3. Add the avx-vendor-cert-scep-agent and avx_platform_gateway_external in ENABLED_PLUGINS in the appviewx.conf file.
4. Specify the datacenter (DC) where the gateway must be deployed:
   - avx_vendor_cert_scep_agent=<dc name>
   - avx_platform_gateway_external=<dc name>
5. Run the <plugins_install.sh>
6. Verify if SCEP is enabled by running kubectl get pods -A | grep scep

```
appviewx@pm-saas-node33:~$ kubectl get pods -A | grep scep
absecon              avx-vendor-cert-scep-agent-6fd76c86b4-hs2hq              3/3     Running     0              8d
appviewx@pm-saas-node33:~$
```

7. Verify the plugin status and port number by running:

```
kubectl get services -A | grep scep
```

8. Make sure that the avx-vendor-cert-scep-agent and avx-vendor-cert-scep-agent are running.

```
appviewx@pm-saas-node33:~$ kubectl get svc -A | grep scep
absecon              avx-vendor-cert-scep-agent              ClusterIP   10.96.221.230   <none>        5312/TCP
external-system      avx-platform-gateway-scep               NodePort    10.101.212.88   <none>        5302:30022/TCP
appviewx@pm-saas-node33:~$
```

9. Make sure that the port number is 5303:30022 in avx-platform-gateway-est.

Note: The number 30022 must be used in the UI configuration.

10. Identify the nodes running the SCEP services by using:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
<kubectl get pods -n external-system -o wide>
```

```
-bash-4.2$ kubectl get pods -n external-system -o wide
NAME                                    READY   STATUS          RESTARTS   AGE   IP              NODE
avx-platform-gateway-676f67587b-54jj8   1/1     Running         5          64d   10.244.198.136  trialnode2.appviewx.net
avx-platform-gateway-676f67587b-h6xrf   1/1     Running         4          62d   10.244.251.30   trialnode3.appviewx.net
avx-platform-gateway-676f67587b-tbqcs   0/1     NodeAffinity    0          64d   <none>          trialnode3.appviewx.net
-bash-4.2$
```

SCEP is available on all the nodes where the external system runs.

For SaaS

HTTPS gateway must be enabled while installing the cloud connector (CC). To do this:

1. Navigate to the installation directory of the cloud connector software.
2. Run:

```
cd deps/tools
```

3. Run:

```
./k3s kubectl get svc -A
```

Note: Ensure that avx-mid-server-gateway-http is present under namespace cc.

Configuring SCEP Endpoint

1. Click (**Menu**) > **CERT+** > **Administration** > **Auto Enrollment** > **SCEP**.
   The **Auto Enrollment : SCEP** page appears.
2. Click the **+ Add** button.
3. Enter the following fields:

Field description on Auto Enrollment : SCEP page

Field	Description
Endpoint Details	
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	**For Onprem** **Without load balancer:**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	FQDN: • **HTTP:** Must contain the FQDN of the node where the external gateway is running. To get the details, run `kubectl get pods -n external-system -o wide`. If the external gateway is running on multiple nodes, you can specify any one of those nodes. • **HTTPS:** Must be same as the web URL. **With load balancer:** **HTTP:** • **FQDN:** Must be the FQDN of the load balancer. **For SaaS:** **Using On-premises CC:** **Without load balancer** • **FQDN:** Must be the **FQDN** of the cloud connector where the auto-enrollment gateway is running. **With load balancer** • **FQDN:** Must be the FQDN of the load balancer. **Using Direct Gateway** In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***SCEP URL**	Select either HTTP or HTTPS. Based on the selection of this field, the SCEP endpoints will be configured with HTTP or HTTPS URL. The port information will be dynamically updated based on this selection. **Using Direct Gateway** In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use HTTPS.
***Port**	**For Onprem**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Without load balancer:
	• **Port:**
	  • **HTTP:** By default, it is port 30022. Leave it as is.
	  • **HTTPS:** By default, it is port 31443. Leave it as is.
	
	With load balancer:
	
	HTTP
	• **Port:** Must be the listening port of the load balancer.
	
	Note:
	• It is recommended to set the listening port as 30022, which is the same as AppViewX.
	• If the load balancer's listening port is different from 30022, then update the respective port.
	
	For SaaS:
	
	Using On-premises CC:
	
	Without load balancer
	• **Port:**
	  • **HTTP:** By default, it is port 30022. Leave it as is.
	  • **HTTPS:** By default, it is port 30020. Leave it as is.
	
	With load balancer
	• **Port:** Must be the listening port of the load balancer.
	
	Note:
	• It is recommended to set the listening port as 30022, which is the same as AppViewX.
	• If the load balancer's port is different from 30022, then update the respective port.
	
	Using Direct Gateway

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the SaaS setup, to use the direct AEP gateway without installing the cloud connector, use only port 443.
Challenge Password	A challenge token to be used while enrolling certificates. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, it is recommended to provide a challenge password.
CA Accounts	
***Certificate Group**	Select a specific group under which certificate needs to be enrolled.
***Certificate Category**	Select a specific certificate type (Server / Client) to be enrolled.
***Select CA**	Select the required CA from the available options. The certificate will be enrolled under the selected CA. The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS • AppViewX PKIaaS Native • Amazon Private CA • DigiCert • DigiCert One • EJBCA • Entrust • Entrust MPKI • GlobalSign Atlas • GlobalSign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust • Sectigo (Commodo Certificate Manager) • SwissSign

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The Vendor Specific Details and Custom Attributes section are displayed for some of the CAs as follows: • DigiCert • EJBCA • Entrust • Entrust MPKI • GlobalSign MSSL • MS Enterprise • Nexus
***:** mandatory fields.	

Note: Use the port number that is appearing when you enable SCEP services.

Health check URL for load balancer:

Onprem

a. **HTTP method:** GET
b. **Healthcheck API:** https://<FQDN>:30022
   i. **FQDN:** FQDN of the external gateway running nodes.
   ii. **Expected response code:** 404. As the load balancer is accessing the URL without any parameters, it will receive a 404 response.

SaaS

- **HTTP method:** GET
- **Healthcheck API:** https://<FQDN>:30022 (HTTP) / https://<FQDN>:30020 (HTTP)
- **FQDN:** FQDN of cloud connector enabled with the HTTP/HTTPS gateway.
- **Expected response code:** 404. As the load balancer is accessing the URL without any parameters, it will receive a 404 response.

When **AppViewX** is selected as CA. The fields for AppViewX CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with the SCEP client machine.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **AppViewX PKIaaS Native** is selected as CA. The fields for AppViewX PKIaaS Native are as follows:

Details for AppViewX PKIaaS Native - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Template Name	Select a template name from the dropdown list.
***Issuer Name**	Select an issuer name to issue the certificate.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. **Note:** For some CAs, the validity available in their respective CA portal is considered despite the specified certificate validity.
*: mandatory fields.	

When **Amazon Private CA** is selected as CA. The fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the group's associated policy. Select an appropriate value as required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **AppViewX PKIaaS** is selected as CA. The fields for AppViewX PKIaaS CA are as follows:

Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with the SCEP client machine.
***Issuer Location**	Select the issuer location associated with the CA.
***Issuer Name**	Select the issuer name used to issue the certificate.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **DigiCert** is selected as CA. The fields for Digicert CA are as follows:

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Division**	Select a division associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Certificate Type**	Select a valid certificate type associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Order Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

If the **Select CA =DigiCert**, then a separate section **Vendor Specific Details** is displayed after the CA Accounts section with two fields described below.

Vendor Specific Details for Digicert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type. The dropdown is populated with the first available value. Select an appropriate value as required.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with the account balance. Returns an error if this option is disabled for the account or if the account has an insufficient fund. • **Bill To Default Credit Card** - Pay with the account's default credit card. Returns an error if no default credit card is configured for the account
*: mandatory fields.	

When **DigiCert One** is selected as CA. The fields for DigiCert One CA are as follows:

Details for DigiCert One CA - Field Description Table

Fields	Description
***CA Account Name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server or Client.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Proxy Required	Enable this field if the CA communication needs to happen via proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center for CA communication, with the CC node being the recommended option. The selected node will handle the communication through the chosen CC node.
CA Configuration	
***Base URL**	This URL will contain the hostname of the DigiCert CA instance and used for constructing the API requests.
***Authentication method**	By default, API Token is selected.
***API Token**	Enter the API token to authorize the communication between AppViewX and DigiCert One.
Allow Seat ID during enrollment	Enabling this field displays a Seat ID field in the Auto enrollment settings that you can use instead of the CA settings.
***Seat ID**	Unique value assigned to identify an entity in the DigiCert One account.You can provide multiple ID separated by a comma. They can be used for enrollment, renewal, and regeneration.
Use DigiCert One to switch certificates from DigiCert MPKI	Enable this field to automatically switch your DigiCert MPKI certificates to DigiCert One with auto-enrollment/auto-regenerate.
***: mandatory fields.	

When **EJBCA** is selected as CA. The fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA’s issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
*: mandatory fields.	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
*: mandatory fields.	

When **Entrust** is selected as CA. The fields for Entrust CA are as follows:

Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Certificate Type**	Select a valid certificate type associated with the CA account. • If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. • If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the requester name.
Requester Email	Enter a valid email ID.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Requester Phone	Enter the 10-digit phone number.
***: mandatory fields.	

When **Entrust MPKI** is selected as CA. The fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***: mandatory fields.	

If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section. The fields for Vendor specific details are as follows:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Certificate Profile**	Select a certificate profile from the dropdown list.
***: mandatory fields.	

When **GlobalSign Atlas** is selected as CA. The fields for GlobalSign Atlas CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for GlobalSign Atlas CA - Field Description Table

Fields	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.
Certificate Profile	Select the certificate Profile from the dropdown list.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

A **Generic Fields** section is also displayed below the **CA Accounts** section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.

When **GlobalSignMSSL** is selected as CA. The fields for GlobalSign MSSL CA are as follows:

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
*: mandatory fields.	

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
*: mandatory fields.	

When **Google** is selected as CA. The fields for Google CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
Template Name	Select an appropriate template name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **HydrantID** is selected as CA. The fields for HydrantID CA are as follows:

Details for HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **IDnomic** is selected as CA. The fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: mandatory fields.	

When **Microsoft Enterprise** is selected as CA. The fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed with a **Template Name** dropdown after the CA Accounts section.

When **Microsoft Standalone** is selected as CA. The fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

When **Nexus** is selected as CA. The fields for Nexus CA are as follows:

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
***Procedure**	Select the procedure based on the configurations made in the Certificate Authority Setting.

When **OpenTrust** is selected as CA. The fields for OpenTrust CA are as follows:

Details for OpenTrust CA - Field Description Table

Fields	Description
***CA Account name**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Management Profile**	Select the certificate issuance policy defined in OpenTrust CA.
Zone	The AppViewX configuration wrapper that maps to a CA + profile, and is used by end-users or automation to request certificates consistently.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

When **Sectigo (Comodo Certificate Manager)** is selected as CA. The fields for Sectigo (Comodo Certificate Manager) CA are as follows:

Details for Sectigo (Comodo Certificate Manager) CA - Field Description Table

Fields	Description
***CA Account**	A unique name to identify the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Certificate Type**	Select a value from the dropdown list.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

Details for SwissSign CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate creation operations.
***Client Name**	Select the specific client.
***Product**	Select the specific product.
***Registration Authority Certificate**	Add the chosen CA's issued server certificate with the private key. This certificate acts as the RA certificate for SCEP enrollments. Search the required certificate from the AppViewX server inventory by typing the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":"

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

4. Configure the **Advanced Settings** details as follows:

   The following table provides the field description for Advanced Settings:

Advanced Settings - Field Description Table

Fields	Description
***Include Truststore Certificates**	Select whether the issuer certificate needs to be sent to client machines after enrollment.
***Fetch Certificate Parameters**	Select *Yes* or *No*. Setting the radio button to *Yes* enables the system to automatically fetch certificate parameters from a Suggestive Policy and append them to the client CSRs.
High Speed Transactions	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol's Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page. **Note:** By default, this field is set to **Yes** for AppViewX PKIaaS CA.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed. • If it is set to **No**, then the AppViewX will do the default behavior of enrolling a new certificate for each request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Retry Count**	Based on this value, the SCEP agent will trigger the number of calls to collect the certificate from AppViewX until it is received. Values accepted between 5 - 99.
***Retry Frequency**	The value specified in this field determines the duration taken between the trigger calls by the SCEP agent. Values accepted between 10 - 99.
***Certificate Poll Type**	Select *Issuer and Subject* or *Transaction ID*. The client agent will use this field to poll the issued certificate from the agent to the subsystem certificate plugin.
Duplicate Certificate Migration	Selecting this check-box will cause the previously issued certificates for the same CSR parameters to be revoked and deleted from AppViewX. **Note:** By default, this field is enabled for AppViewX PKIaaS CA.
*: mandatory fields.	

5. Click **Save**.

Validating SCEP

1. Configure the SCEP endpoint in AppViewX GUI using the preceding steps.
2. The agent configuration should be in **valid** status.

3. If the above steps are completed, then refresh the following URL from the web browser

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. <scep endpoint URL from appviewx GUI>?operation=GetCACaps

b. **Expected response:** In the browser window, you should see the following data:

```
Unset
AES9
DES3
GetNextCACert
POSTPKIOperation
Renewal
SHA-1
SHA-256
SCEPStandard
```

If you get the above response, then you can confirm that AppViewX is working fine.

Enrolling and Renewing Certificates via SCEP

The following conditions must be met, if the SCEP client sends a CSR to AppViewX SCEP Server for a certificate renewal:

1. If the signing certificate is self-signed, then validate if the subject name in the self-signed certificate matches with the common name in the CSR subject.
   a. If it matches, then AppViewX will proceed with enrollment.
   b. If it does not match, then validate whether the challenge passphrase is configured for the endpoint and is validated by the application.

   Note: If the device enrollment uses a self-signed certificate, it is advised to configure challenge passphrase as part of the endpoint. This must be configured on the SCEP client side for any enrollment.

2. If the request is signed with an RA certificate (as configured in AppViewX SCEP endpoint) then AppViewX will proceed with the enrollment.
3. If the signer certificate is any other certificate in the inventory, then check if this certificate belongs to the same entity by doing the common name match. Check if the common name of the signer certificate and the common name in the CSR subject, if it matches, then it is considered as renewal and the certificate is issued.
4. If the signer certificate is any other certificate in the inventory and its common name doesn't match with the common name in the CSR subject, then the certificate request is rejected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

MS Intune

- Configuring AppViewX MS Intune Server
- Configuring AppViewX MS Intune Client

What is MS Intune?

MS Intune or **Microsoft Intune** is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). AppViewX has a SCEP based integration with MS Intune. This integration provides for provisioning of certificates to Microsoft Intune managed mobile devices.

- There should be an agent (avx_vendor_cert_intune_agent) up and running for MS Intune in AppViewX.
- This Intune plugin can either be in HTTPS or HTTP, but it needs a HTTP gateway running in order to communicate with the client.
- In order to make that HTTP gateway up and running go to /home/appviewx/appviewx/avxgw/avxgw-profile.json. Enable the HTTP profile and restart the gateway.
- It is highly recommended to keep the 'Approval Required' flag in OFF state from **Menu > Inventory > Certificate > Policy** page.
- A valid agent settings should be available in **Menu > Inventory > Certificate > Settings**.

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). Intune is integrated with Microsoft's Enterprise Mobility + Security (EMS) suite, it manages the application and protects the organization data. Users can configure specific policies to control the applications. It makes sure that the organization data is protected and isolated from the personal data.

What is SCEP?

Simple Certificate Enrollment Protocol (SCEP) is a protocol that allows devices to enroll for a certificate using URL and a shared secret to communicate with a PKI. It uses the CA certificate to secure the message exchange for the CSR. SCEP is used for Certificate-based authentication, whereby access to services such as Wi-Fi, VPN, and securing e-mail through encryption is carried out using certificates.

What is MS Intune Connector?

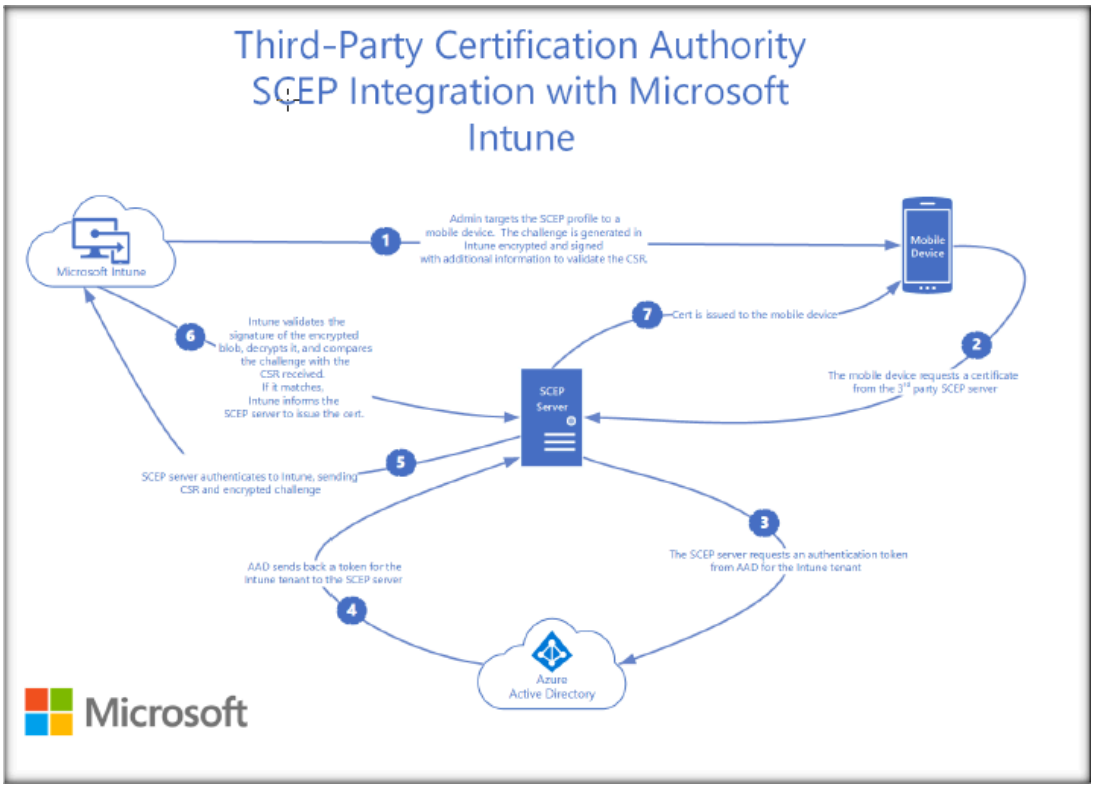
MS Intune AppViewX Connector is a SCEP server that handles certificate request validation through Microsoft Intune and certificate enrollment through AppViewX. To use the SCEP for certificates in Intune

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. In Intune, the administrator creates a SCEP certificate profile, and then targets the profile to users or devices.
2. The device checks into Intune.
3. Intune creates a unique SCEP challenge. It adds the additional integrity-check information, such as what the expected subject and SAN should be.
4. Intune encrypts and signs both the challenge and integrity-check information, and then sends this information to the device with the SCEP request.
5. The device generates a certificate signing request (CSR) and a public/private key pair on the device based on the SCEP certificate profile that is pushed from Intune.
6. The CSR and encrypted/signed challenge are sent to the third-party SCEP server endpoint.
7. The SCEP server sends the CSR and the challenge to Intune. Intune then validates the signature, decrypts the payload, and compares the CSR to the integrity-check information.
8. Intune sends back a response to the SCEP server and states whether the challenge validation is successful or not.
9. If the challenge is successfully verified, then the SCEP server issues the certificate to the device.

The following illustration shows the end-to-end flow of the device certificate enrollment via Microsoft Intune with help of SCEP server and third-party CA.

Figure 4. End-to-End Flow of the Device Certificate Enrollment



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

MS Intune AppViewX connector plays the role of the third-party SCEP server that enables certificate enrollment through AppViewX. This SCEP server performs as follows:

1. Handles the GetCACaps SCEP request by providing the capabilities that are supported by the CA.
2. Handles the GetCACert SCEP request by providing the SCEP server certificate.
3. Handles the certificate enrollment SCEP request by performing the below steps:
   a. Validates the incoming enrollment requests using the Microsoft java library.
   b. If the validation is successful, get the certificate issued by AppViewX and send it back to the device.
   c. Send appropriate (success/failure) notifications to Intune using the Microsoft library.

Managing devices using MS Intune

In Intune, users can manage the devices using a systematic approach that is required for the organization. The organization-owned devices may require full control on the devices that include settings, features, and security. In this approach, devices and users of these devices **enroll** to Intune. Once enrolled, they receive predefined rules and settings through policies configured in Intune. For example, you can set credentials, security threat protections, create VPN connections and so on.

When devices are enrolled and managed in Intune, administrators can:

- Check the devices enrolled and get an inventory of devices accessing organization resources.
- Configure the devices to set security and health standards for organization. For example, blocking the jail-broken devices.
- Push certificates to devices so users can easily access your Wi-Fi network or use a VPN to connect to your network.
- Check the reports on users and devices that are compliant, and not compliant.
- Remove the organization data if a device is lost, stolen, or not in use.

Third-party CA or RAs can provision mobile devices with new or renewed certificates by using the simple certificate enrollment protocol (SCEP).

What's Next?

Configuring AppViewX MS Intune Server

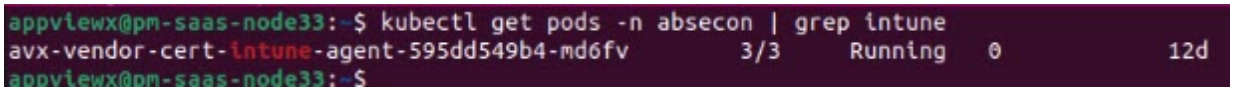
Prerequisites

Onprem

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

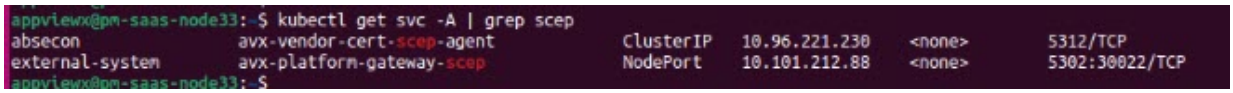
- Make sure that the Intune pod is running in the cluster by using the command:

```
kubectl get pods -A | grep intune
```



- Make sure that <avx-platform-gateway-scep> is running in the cluster by using the command:

```
kubectl get svc -A | grep scep
```



SaaS

HTTPS gateway must be enabled while installing the cloud connector (CC). To do this:

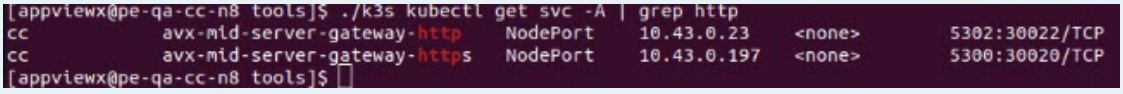
1. Navigate to the installation directory of the cloud connector software.
2. Run

```
cd deps/tools
```

3. Run

```
./k3s kubectl get svc -A | grep http
```

Note: It should have the avx-mid-server-gateway-http or avx-mid-server-gateway-https under namespace cc.



Enabling MS Intune Services

For Onprem

1. Log onto the AppViewX installer node. Open the terminal window.
2. Go to </installation_folder/appviewx_kubernetes/scripts> folder.
3. Add the avx-vendor-cert-intune-agent and avx_platform_gateway_external in ENABLED_PLUGINS in the appviewx.conf file.
4. Specify the datacenter (DC) where the gateway must be deployed:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- avx_vendor_cert_intune_agent=<dc name>
- avx_platform_gateway_external=<dc name>

5. Run the <plugins_install.sh>
6. Verify if Intune is enabled by running kubectl get pods -A | grep intune

```
appviewx@pm-saas-node33:~$ kubectl get pods -A | grep intune
absecon                avx-vendor-cert-intune-agent-595dd549b4-xkjxg            3/3
appviewx@pm-saas-node33:~$
```

7. Verify the plugin status and port number by running:

```
kubectl get svc -A | grep scep
```

```
appviewx@pm-saas-node33:~$ kubectl get svc -A | grep scep
absecon                avx-vendor-cert-scep-agent           ClusterIP   10.96.221.230   <none>        5312/TCP
external-system        avx-platform-gateway-scep            NodePort    10.101.212.88   <none>        5302:30022/TCP
appviewx@pm-saas-node33:~$
```

Make sure that the avx-platform-gateway-scep is running and the port number is 5303:30022 in avx-platform-gateway-scep.

Note: The number 30022 must be used in the UI configuration.

8. Identify the nodes running the SCEP services by using:

```
<kubectl get pods -n external-system -o wide>
```

```
NAME                                    READY   STATUS         RESTARTS   AGE   IP              NODE
avx-platform-gateway-676f67587b-54jj8   1/1     Running        5          64d   10.244.198.136  trialnode2.appviewx.net
avx-platform-gateway-676f67587b-h6xrf   1/1     Running        4          62d   10.244.251.30   trialnode3.appviewx.net
avx-platform-gateway-676f67587b-tbqcs   0/1     NodeAffinity   0          64d   <none>          trialnode3.appviewx.net
-bash-4.2$
```

SCEP is available on all the nodes where the external system runs.

For SaaS

HTTP/HTTPS gateway must be enabled while installing the cloud connector (CC). To do this:

1. Navigate to the installation directory of the cloud connector software.
2. Run:

```
cd deps/tools
```

3. Run:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
./k3s kubectl get svc -A
```

Note: Ensure that avx-mid-server-gateway-http is present under namespace cc.

Configuring AppViewX MS Intune Server

To conduct mobile device certificate enrollments for MS Intune managed devices using the MS Intune protocol (SCEP-based) on AppViewX, the administrator or the privileged user must initially configure the MS Intune server agent using the AppViewX portal. Once the MS Intune server agent is successfully set up through the portal, a URL will be generated. Clients can then use this URL to submit enrollment requests to AppViewX via MS Intune.

1. Go to **(Menu)** > **Cert+** > **Administration** > **Auto Enrollment** > **MS INTUNE**.
2. Click **Configure Now** or **+Add** icon.
3. Configure the **End Point Details** as follows:

   Prerequisites for entering the IP/FQDN field:

   - For SaaS
     - The **Cloud Connector Name** (in the Add Cloud connector page) must be the same as the FQDN name entered.
     - If the customer is using LB on top of multiple CC, then the FQDN of the LB should be used.
   - For On-Prem
     - The IP / FQDN of the machine where the external gateway is running.
     - If the customer is using LB on top of multiple CC then the FQDN of the LB should be used.
   - The given FQDN must be resolvable in the cloud connector machine and also in the company portal Application running machine
   - The CC should have the reachability to the Endpoint.

   The fields for Endpoint Details are as follows:

Endpoint Details - Field Description Table

Fields	Description
***Name**	A unique name (alphanumeric string) to identify the agent setting. Name should not start with special characters. Acceptable characters: A-Z, a-z, 0-9, '.', '_', '-'
***IP/FQDN**	**For Onprem** **Without load balancer:**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	FQDN: • **HTTP:** Must contain the FQDN of the node where the external gateway is running. To get the details, run `kubectl get pods -n external-system -o wide`. If the external gateway is running on multiple nodes, you can specify any one of those nodes. • **HTTPS:** Must be same as the web URL. **With load balancer:** • **FQDN:** Must be the FQDN of the load balancer. **For SaaS:** **Using On-premises CC:** **Without load balancer** • **FQDN:** Must be the FQDN of the cloud connector where the auto-enrollment gateway is running. **With load balancer** • **FQDN:** Must be the FQDN of the load balancer. **Using Direct Gateway** In the SaaS setup, to use the direct AEP gateway without installing the cloud connector, the FQDN/IP address will be the tenant URL with "-aep" before the domain name. The format is as follows: <tenant>-aep.<domainname>.
***Intune URL**	Select either HTTP or HTTPS. Based on the selection of this field, the Intune endpoints will be configured with HTTP or HTTPS URL. The port information will be dynamically updated based on this selection. **Using Direct Gateway** In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, use HTTPS.
***Port**	**For Onprem**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description

	Without load balancer:
	• **Port:**
	  • **HTTP:** By default, it is port 30022. Leave it as is.
	  • **HTTPS:** By default, it is port 31443. Leave it as is.
	
	With load balancer:
	
	HTTP
	• **Port:** Must be the listening port of the load balancer.
	
	Note:
	• It is recommended to set the listening port as 30022, which is the same as AppViewX.
	• If the load balancer's listening port is different from 30022, then update the respective port.
	
	For SaaS:
	
	Using On-premises CC:
	
	Without load balancer
	• **Port:**
	  • **HTTP:** By default, it is port 30022. Leave it as is.
	  • **HTTPS:** By default, it is port 30020. Leave it as is.
	
	With load balancer
	• **Port:** Must be the listening port of the load balancer.
	
	Note:
	• It is recommended to set the listening port as 30022/30020, which is the same as AppViewX.
	• If the load balancer's port is different from 30022/30020, then update the respective port.
	
	Using Direct Gateway

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	In the SaaS setup, to use the direct AEP gateway without installing the cloud connector, use only port 443.
Proxy Required	Select the checkbox if required. If enabled, the communication with the Azure portal to validate the challenge password will go via the proxy details provided in the general settings. It is used to perform the challenge verification in Intune, via the proxy server (if there is no internet connectivity).
***Data Center**	The communication with the Azure portal to validate challenge password will go via the CC in the datacenter. Internet connectivity for the CC is mandatory. In the SaaS setup, to consume the direct AEP gateway without installing the cloud connector, select **cloud-dc** (it is the only available value for this configuration).
***: mandatory fields.	

4. Configure the **Intune Details**.

Intune Details - Field Description Table

Fields	Description
***Client ID**	Client ID of the Intune Account - this value should have been captured during Intune App Registration.
***Tenant ID**	Tenant ID is the domain name in your account ID. For example, if your account id is **admin@test.onmicrosoft.com**, then the tenant ID is **test.onmicrosoft.com**.
***Client Secret**	Client Secret for the Intune Account - this value should have been captured during Intune App Registration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Cloud Type**	Select any of the options: • **Azure Public:** This is the most common and traditional deployment model in which Azure's resources are owned and operated by Microsoft sharing them across multiple tenants. • **Azure Government:** This is a specialized version of Azure designed to meet the specific regulatory and compliance needs of government agencies in the US. It is isolated from the public Azure cloud and provides the highest level of security.
***: mandatory fields.	

Health check URL for load balancer:

Onprem

- **HTTP method:** GET
- **Healthcheck API:** https://<FQDN>:30022
- **FQDN:** FQDN of the external gateway running nodes.
- **Expected response code:** 404. As the load balancer is accessing the URL without any parameters, it will receive a 404 response.

SaaS

- **HTTP method: GET**
- **Healthcheck API:** https://<FQDN>:30022 (HTTP) (or) https://<FQDN>:30020 (HTTPS)
- **FQDN:** FQDN of cloud connector enabled with the HTTP/HTTPS gateway.
- **Expected response code:** 404. As the load balancer is accessing the URL without any parameters, it will receive a 404 response.

5. Configure the **CA Accounts** as follows:

CA Accounts - Field Description Table

Fields	Description
Certificate Group	Select a specific group under which certificate needs to be enrolled.
Certificate Category	Select a specific certificate type (Server / Client) to be enrolled.
Select CA	Select the required CA from the available options. The certificate will be enrolled under the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	The CAs associated with the Default certificate group are: • AppViewX • AppViewX PKIaaS • AppViewX PKIaaS Native • Amazon Private CA • DigiCert • DigiCert One • EJBCA • Entrust • Entrust MPKI • Globalsign Atlas • Globalsign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust • Sectigo (Comodo Certificate Manager) • SwissSign **Note:** The Vendor Specific Details section is displayed only after the following CA Account is selected: • DigiCert • EJBCA • Entrust • Entrust MPKI • GlobalSign MSSL • Microsoft Enterprise • Nexus
***: mandatory fields.	

When **AppViewX** is selected as CA, the fields for AppViewX CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for AppViewX CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with SCEP client machine.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **AppViewX PKIaaS Native** is selected as CA. The fields for AppViewX PKIaaS Native are as follows:

Details for AppViewX PKIaaS Native - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Template Name	Select a template name from the dropdown list.
***Issuer Name**	Select an issuer name to issue the certificate.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. **Note:** For some CAs, the validity available in their respective CA portal is considered despite the specified certificate validity.
*: mandatory fields.	

When **AppViewX PKIaaS** is selected as CA, the fields for AppViewX PKIaaS CA are as follows:

Details for AppViewX PKIaaS CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with the SCEP client machine.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Issuer Name**	Select an issuer name to issue the certificate.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***CA Certificate**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with MSIntune client machine.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*****: mandatory fields.	

When **Amazon Private CA** is selected as CA, the fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Region**	Select a valid region associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown list is populated with the first available value from the group's associated policy. Select an appropriate value as required.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

When **DigiCert** is selected as CA, the fields for DigiCert CA are as follows:

Details for DigiCert CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Division**	Select a division associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Certificate Type**	Select a valid cert type associated with the CA account. The dropdown list is populated with the first available value. Select an appropriate value as required.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Order Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section. The fields for Vendor specific details are as follows:

Vendor Specific Details for DigiCert CA - Field Description Table

Fields	Description
***Server Type**	Select a server type.
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
***: mandatory fields.	

When **DigiCert One** is selected as CA. The fields for DigiCert CA are as follows:

Details for DigiCert One CA - Field Description Table

Fields	Description
***CA Account Name**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names shouldnot start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server or Client.
Proxy Required	Enable this field if the CA communication needs to happen via proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center for CA communication, with the CC node being the recommended option. The selected node will handle the communication through the chosen CC node.
CA Configuration	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Base URL**	This URL will contain the hostname of the DigiCert CA instance and used for constructing the API requests.
***Authentication method**	By default, API Token is selected.
***API Token**	Enter the API token to authorize the communication between AppViewX and DigiCert One.
Allow Seat ID during enrollment	Enabling this field displays a Seat ID field in the Auto enrollment settings that you can use instead of the CA settings.
***Seat ID**	Unique value assigned to identify an entity in the DigiCert One account.You can provide multiple ID separated by a comma. They can be used for enrollment, renewal, and regeneration.
Use DigiCert One to switch certificates from DigiCert MPKI	Enable this field to automatically switch your DigiCert MPKI certificates to DigiCert One with auto-enrollment/auto-regenerate.
*: mandatory fields.	

When **EJBCA** is selected as CA, the fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
*: mandatory fields.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section. The fields for Vendor specific details are as follows:

Vendor Specific Details for EJBCA CA - Field Description Table

Fields	Description
***End Entity Profile Name**	Select a profile of an end entity.
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.
*: mandatory fields.	

When **Entrust** is selected as CA. The fields for Entrust CA are as follows:

Details for Entrust CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select a valid certificate type associated with the CA account. • If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. • If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: mandatory fields.	

If the selected CA is **Entrust**, a separate section displaying **Vendor specific details** and **Custom Attributes** is displayed after the **CA Accounts** section.

Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Vendor Specific Details for Entrust CA - Field Description Table

Fields	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the requester name.
Requester Email	Enter a valid email ID.
Requester Phone	Enter the 10-digit phone number.
*: mandatory fields.	

When **Entrust MPKI** is selected as CA, the fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the selected CA is **Entrust MPKI**, a separate section **Vendor specific details** is displayed after the **CA Accounts** section.

The fields for Vendor specific details are as follows:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Fields	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.
*: mandatory fields.	

When **GlobalSign Atlas** is selected as CA, the fields for GlobalSign Atlas CA are as follows:

Details for GlobalSign Atlas CA - Field Description Table

Fields	Description
***Select CA**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
API Credential Friendly name	Select a CA Account to communicate with during the certificate enrollment actions.
Certificate Profile	Select the certificate Profile from the dropdown list.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.

When **GlobalSignMSSL** is selected as CA, the fields for GlobalSign MSSL CA are as follows:

Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
CA Account	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.
*: mandatory fields.	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint will be registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Fields	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.
*: mandatory fields.	

When **Google** is selected as CA, the fields for Google CA are as follows:

Details for Google CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Certificate Profile**	Select the certificate profile type.
***Issuer Location**	Select an issuer location that is associated with the CA account.
***Pool Name**	Select a pool name to issue the certificate.
Template Name	Select an appropriate template name to issue the certificate.
***Issuer Name**	Select an issuer name to issue the certificate.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
*: mandatory fields.	

When **HydrantID** is selected as CA, the fields for HydrantID CA are as follows:

Details for HydrantID CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***** **CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

When **Microsoft Enterprise** is selected as CA, the fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

If the selected CA is Microsoft Enterprise, a separate section **Vendor specific details** is displayed after the CA Accounts section with a dropdown field - **Template Name** - Select a template from the dropdown list.

When **IDnomic** is selected as CA, the fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

When **Microsoft Standalone** is selected as CA, the fields for Microsoft Standalone CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for Microsoft Standalone CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

The following table provides the field description for **Nexus CA**:

Details for Nexus CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate-creation operations.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields.	

When **OpenTrust** is selected as CA. The fields for OpenTrust CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for OpenTrust CA - Field Description Table

Fields	Description
***CA Account name**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Management Profile**	Select the certificate issuance policy defined in OpenTrust CA.
Zone	The AppViewX configuration wrapper that maps to a CA + profile, and is used by end-users or automation to request certificates consistently.
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
*: mandatory fields.	

A **Profile Parameters** section is also displayed below the CA Accounts section. It contains the fields such as **Common Name*, *Organizational Unit*, **Organization*, **Email*, **Password*. or as configure in the Certificate Authority settings page.

When **Sectigo (Comodo Certificate Manager)** is selected as CA. The fields for Sectigo (Comodo Certificate Manager) CA are as follows:

Details for Sectigo (Comodo Certificate Manager) CA - Field Description Table

Fields	Description
***CA Account**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Certificate Type**	Select a value from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Server Certificate**	Select the chosen CA-issued certificate, using which the trusted inventory is validated. Type the exact common name or serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).
*: mandatory fields	

When **SwissSign** is selected as CA. The fields for SwissSign CA are as follows:

Details for SwissSign CA - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate creation operations.
***Client Name**	Select the specific client.
***Product**	Select the specific product.
***Server Certificate**	Select the certificate issued by the selected CA using which the trusted inventory is validated. You can search for it by typing the exact common name or the serial number. **Note:** You can search for certificates using the serial number with or without colon ":".
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.
*: mandatory fields.	

6. Configure the **Advanced Settings**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The fields in the Advanced Settings section are as follows:

Advanced Settings - Field Description Table

Fields	Description
***Fetch Certificate Parameters**	Select Yes or No Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.
***Retry Count**	Based on this value, the EST agent will trigger the number of calls to collect the certificate from AppViewX until it is received. Values accepted between 5 - 99.
***Retry Frequency**	The value specified in this field determines the duration taken between the trigger calls by the EST agent. Values accepted between 10 - 99.
***Certificate Poll Type**	Select *Issuer and Subject* or *Transaction ID*. The client agent will use this field to poll the issued certificate from the agent to the subsystem certificate plugin.
***High Speed Transactions**	Based on the selection of this field, the endpoint will be configured with or without High Performance transaction times. ACME protocol's Revocation actions are not supported in High Performance mode. Request information pertaining to High-Performance can be viewed on the Direct Requests page. **Note:** By default, this field is set to **Yes** for AppViewX PKIaaS CA.
***Return Existing Certificate**	If this option is enabled (**Yes**) then for request with AppViewX should check and return the existing valid certificate for the same CSR & public key from inventory if available otherwise it should proceed with enrollment and return the certificate. • If it is set to **Yes**, the Certificate Threshold field is displayed. • If it is set to **No**, then the AppViewX will do the default behavior of enrolling a new certificate for each request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Duplicate Certificate Migration	Selecting this check-box will cause the previously issued certificates for the same CSR parameters to be revoked and deleted from AppViewX. **Note:** By default, this field is enabled for AppViewX PKIaaS CA.
***Mitigate Certificates issued within**	This field is enabled only when the **Duplicate Certificate Migration** check-box is selected.
***: mandatory fields.	

7. Click **Save**.

Validating MS Intune

1. Configure the MS Intune endpoint in AppViewX GUI using the preceding steps.
2. The agent configuration should be in **valid** status.

3. If the above steps are completed, then refresh the following URL from the web browser:
   a. <intune endpoint URL from appviewx GUI>?operation=GetCACaps
   b. **Expected response:** In the browser window, you should see the following data:

```
Unset
        AES
        DES3
        SHA-1
        SHA-256
        POSTPKIOperation
```

If you get the above response, then you can confirm that AppViewX is working fine.

Configuring AppViewX MS Intune Client

You can configure the AppViewX MS Intune client with the steps detailed in this section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Testing on Windows v10.0 Device

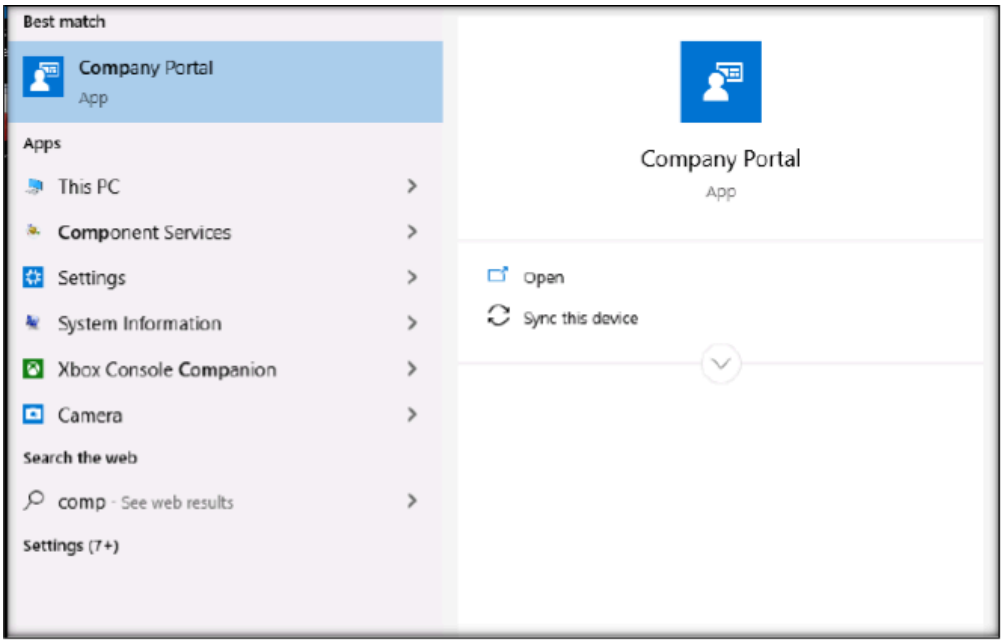
AppViewX MS Intune integration can be tested by enrolling in a Windows v10.0 device. To enroll in other devices, follow the same procedure. To enroll, the Windows v10.0 device must be installed with a **Company Portal** application from the Microsoft Store.

Configuring Windows Accounts Setting

1. Log in to the system that has Windows v10.0 operating system.
2. Open **Settings**.
3. Click **Accounts > Access work or school**.
4. Click **Connect** and confirm your work or school account.
5. Click **Next** to proceed further by providing Azure subscription credentials.
6. Once the account is set, the successful message window is displayed.
7. Click **Done**.

Configuring Company Portal

1. Open the Company Portal application and proceed with the device setup by providing the Azure subscription.



2. Click **Connect** and confirm your work or school account.
3. Provide a valid e-mail address and click **Next** to proceed further to complete the set up.
4. Click **Done**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

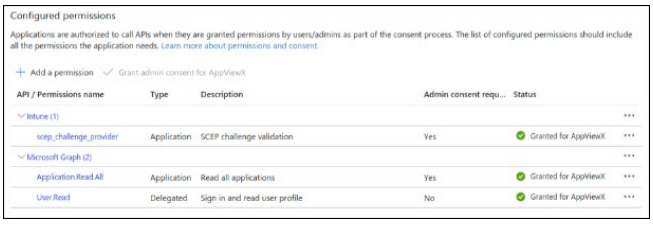
Verifying Enrollment Result

1. Once configuration is completed, the device invokes the GetCACaps, GetCACerts, and PKIRequest (enrollment request) APIs to SCEP server.
2. Monitor the SCEP agent logs in AppViewX and verify that the message ‘AppviewxScepServicePostAction:49 - Response sent successfully for operation: PKIOperation’ occurs in the logs.
3. In the AppViewX application, the newly generated certificate must be shown in the inventory.
4. If the certificate is requested, the device certificate newly generated certificate will be available in the **Server** tab in the certificate inventory.
5. If the certificate is a requested user certificate, the new certificate will be available under the **Client** tab in the certificate inventory.
6. In the Windows device, open the cert store (Windows key+R -> certlm.msc) and make sure that the serial number of the certificate available in the personal cert store matches with the serial number of the certificate that is newly created in AppViewX.

Best Practices

• For auto-enrollment, create a separate certificate group and CA policy in AppViewX.
• During policy creation, select only the required bit-length (minimum 2048-bit).

Troubleshooting

#	Error Message	Description	Troubleshooting
1	Challenge Password Authentication Failed	The issue is either with 1. Not enough API permissions available for the tenant in the Azure portal. 2. Tenant details (Tenant ID, client ID and secret) provided during Intune	Check the following: 1. Tenant needs three API permissions under App registrations in the Azure portal. See the following attached image:  2. Verify the tenant details provided in the Intune endpoint configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
		endpoint configuration in AppViewX GUI might be incorrect.	
2	Given organization must match with organization defined in group policy.	The policy mapped for the MS Intune endpoint configured group is set as strict and organization is configured in the policy. The CSR sent from the client does not contain the exact organization name.	Set the policy as suggestive OR Provided a proper value for Organization in the SCEP profile in MS Intune portal.
3	Failed to submit the certificate to CA	Certificate enrollment has failed from the CA side due to the issue with the submitted CSR.	Check the respective VW request or direct request to find more about the error details and remediate the same.
4	Either CSR parameters,CA details or certificate algorithm values are not compliant with the policy	CSR parameters from the client are not matching with parameters configured in the AppViewX policy.	Check if the policy is set as strict. • Provide a proper value for Organization in the SCEP profile in MS Intune portal. • Change the policy type to Suggestive.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

#	Error Message	Description	Troubleshooting
	name - <Policy Name>		

References

1. Microsoft Docs - Add partner certification authority in Intune using SCEP
2. GitHub - Microsoft/Intune-Resource-Access
3. Simple Certificate Enrollment Protocol - draft-nourse-scep-23
4. Microsoft Docs - Set up Microsoft Intune
5. Microsoft Docs - Set up third-party CA integration

CMP

Certificate Management Protocol (CMP)

Certificate Management Protocol (CMP) is an internet protocol standardized by the Internet Engineering Task Force (IETF) used for obtaining X.509 digital certificates within a public key infrastructure (PKI). Some of the **general constraints** are as follows:

- Out-of-band distribution of authentication keys between RA and CA
  - RA / device should become a registered entity for AppViewX to accept requests from this entity
- Communication Protocol between RA and CA is SSL/TLS over TCP or HTTPS
  - Packet Exchanged are in the form of RFC 4210 and 4211 (Certificate Management Protocol and Certificate Request Message format)
  - All request and responses are digitally signed using certificate or MAC Key exchanged as challenge password
- User can be authenticated with two mechanisms:
  - SSL Certificate
  - Challenge Password
- HTTPS is the protocol used in CMP.
- Default port is 31443.

Certificate Management Protocol supports on-line interactions between PKI components. RA should be support for the following requests as per the standard:

- Initialization Request and Response
- Certification Request and Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Renewal Request and Response
- Revocation Request and Response
- Polling Request and Response

What's Next?

- Configuring AppViewX CMP Server

Configuring AppViewX CMP Server

Prerequisites

Onprem

- Make sure that the following pod is running in the cluster by using the command:

```
kubectl get pods -A | grep cmp
```

SaaS

HTTPS gateway must be enabled while installing the cloud connector (CC). To do this:

1. Navigate to the installation directory of the cloud connector software.
2. Run

```
cd deps/tools
```

3. Run

```
./k3s kubectl get svc -A | grep https
```

Note: It should have the avx-mid-server-gateway-https under namespace cc.

Enabling CMP Services

For Onprem

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Log onto the AppViewX installer node.
2. Go to </installation_folder/appviewx_kubernetes/scripts> folder.
3. Add the avx-vendor-cert-cmp-agent in ENABLED_PLUGINS in the appviewx.conf file.
4. Specify the datacenter (DC) where the gateway must be deployed:
   - avx_vendor_cert_cmp_agent=<dc name>

For SaaS

HTTPS gateway must be enabled while installing the cloud connector (CC). To do this:

1. Navigate to the installation directory of the cloud connector software.
2. Run:

```
cc_installed_path/deps/properties
```

3. Open appviewx.properties and set the following fields as *true:*
   a. AUTO_ENROLL_ENABLED=true
   b. ENABLE_MTLS_PROFILE=true
   c. ENABLE_HTTP_PROFILE=true
   d. ENABLE_HTTPS_PROFILE=true
4. Scale down the avx-mid-server-platform pod.
5. Restart the avx-mid-server-starter pod.

> **Note:** Ensure that avx-mid-server-gateway-https is present under namespace cc.

Configuring AppViewX CMP Server

1. Go to **(Menu)** > **CERT+** > **Administration** > **Auto Enrollment** > **CMP**.
2. Click the **Configure Now** button or **+Add** icon from the middle or top-right of the page respectively.
3. Configure the **Agent Details** as follows:

Agent Details - Field Description Table

Field	Description
***Name**	Unique name to identify the agent setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	No special characters other than '.', '-','_' are allowed. Name should not start with special characters.
***Host**	**For Onprem** • Enter the FQDN address of the AppViewX node gateway. It must be the same as the web URL's hostname. **For SaaS** **Using On-premises CC:** • **Without load balancer:** Hostname must be the hostname of the cloud connector where the auto-enrollment gateway is running. • **With load balancer:** Hostname must be the hostname of the load balancer.
***CMP URL**	Select either HTTP or HTTPS. Based on the selection of this field, the CMP endpoints will be configured with HTTP or HTTPS URL. The port information will be dynamically updated based on this selection.
***Port**	**For Onprem** • By default, it is port 31443. Leave it as is. **For SaaS** **Using On-premises CC** • **Without load balancer:** By default, it is port 30020. Leave it as is. • **With load balancer:** Port must be the listening port of the load balancer. **Note:** • It is recommended to set the listening port as 30020, which is the same as AppViewX. • If the load balancer's listening port is different from 30020, then update the respective port.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

4. Configure the **Client Authentication** details as follows:

Client Authentication - Field Description Table

Field	Description
***Authentication Mode**	This field has two values • MAC • Certificate Based Authentication
***Challenge Password**	This field is enabled when **Authentication Mode = MAC**. Enter the password which is used to authenticate the CMP packet.
***Issuer Certificate**	This field appears when **Authentication Mode = Certificate Based Authentication**. Enter the issuer certificate used to authenticate the client certificate,
***RA Certificate**	This field appears when **Authentication Mode = Certificate Based Authentication**. Enter the common name/ serial number of the RA certificate,
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

Load balancer configuration

It is recommended to set the listening port as 30020, which is the same as AppViewX.

Health check URL for load balancer:

- **HTTP method:** GET
- **Healthcheck API:** https://<FQDN>:30020/
- **Hostname:** Hostname of cloud connector enabled with the HTTPS gateway.
- **Expected response code:** 404. As the load balancer is accessing the URL without any parameters, it will receive a 404 response.

5. Configure the **CA Accounts** details as follows:

The fields for CA Accounts section are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Accounts - Field Description Table

Field	Description
***Certificate Group**	Select a specific group under which certificate needs to be enrolled.
***Certificate Category**	Select a specific certificate type (Server / Client) to be enrolled.
***Select CA**	Select the required CA from the available options: • AppViewX • AppViewX PKIaaS • AppViewX PKIaaS Native • Amazon Private CA • DigiCert • DigiCert One • EJBCA • Entrust • Entrust MPKI • Globalsign • Globalsign Atlas • Globalsign MSSL • Google • HydrantID • IDnomic • Microsoft Enterprise • Microsoft Standalone • Nexus • OpenTrust • Sectigo (Comodo Certificate Manager) • SwissSign

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The Vendor Specific Details and Custom Attributes section are displayed for some of the CAs as follows: • Digicert • EJBCA • Entrust • Entrust MPKI • GlobalSign MSSL • MS Enterprise • Nexus The certificate will be enrolled under the selected CA.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **AppViewX** is selected as CA, the fields for AppViewX CA are as follows:

Details for AppViewX CA - Field Description Table

Field	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with CMP client machine.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

When **AppViewX PKIaaS Native** is selected as CA. The fields for AppViewX PKIaaS Native are as follows:

Details for AppViewX PKIaaS Native - Field Description Table

Fields	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Template Name	Select a template name from the dropdown list.
***Issuer Name**	Select an issuer name to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. **Note:** For some CAs, the validity available in their respective CA portal is considered despite the specified certificate validity.
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

When **Amazon Private CA** is selected as CA, the fields for Amazon Private CA are as follows:

Details for Amazon Private CA - Field Description Table

Field	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Region**	Select a valid region associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Issuer**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value. Select an appropriate value as required.
***Signature Algorithm**	Select a valid issuer associated with the CA account. The dropdown is populated with the first available value from the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	group's associated policy. Select an appropriate value as required.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **DigiCert** is selected as CA, the fields for DigiCert CA are as follows:

Details for DigiCert CA - Field Description Table

Field	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***Division**	Select the division associated with the CA account.
***Certificate Type**	Select certificate type to issue the certificate.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Order Validity**	Validity of the certificate to be enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

If the selected CA is **DigiCert**, a separate section **Vendor Specific Details** is displayed after the **CA Accounts** section.The fields for Vendor specific details are as follows:

Vendor Specific Details for DigiCert CA - Field Description Table

Field	Description
***Server Type**	Select a server type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	Select a payment method. The possible options are: • **Bill To Account Balance** - Pay with account balance. Returns an error if this option is disabled for the account or if the account has insufficient fund. • **Bill To Default Credit Card** - Pay with account's default credit card. Returns an error if no default credit card is configured for the account.
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

When **DigiCert One** is selected as CA. The fields for DigiCert One CA are as follows:

Details for DigiCert One CA - Field Description Table

Fields	Description
***CA Account**	A unique name to identify the CA setting. **Note:** No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. For example, Server or Client.
Proxy Required	Enable this field if the CA communication needs to happen via proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center for CA communication, with the CC node being the recommended option. The selected node will handle the communication through the chosen CC node.
CA Configuration	
***Base URL**	This URL will contain the hostname of the DigiCert CA instance and used for constructing the API requests.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Authentication method**	By default, API Token is selected.
***API Token**	Enter the API token to authorize the communication between AppViewX and DigiCert One.
Allow Seat ID during enrollment	Enabling this field displays a Seat ID field in the Auto enrollment settings that you can use instead of the CA settings.
***Seat ID**	Unique value assigned to identify an entity in the DigiCert One account.You can provide multiple ID separated by a comma. They can be used for enrollment, renewal, and regeneration.
Use DigiCert One to switch certificates from DigiCert MPKI	Enable this field to automatically switch your DigiCert MPKI certificates to DigiCert One with auto-enrollment/auto-regenerate.
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

When **EJBCA** is selected as CA, the fields for EJBCA CA are as follows:

Details for EJBCA CA - Field Description Table

Field	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

If the selected CA is **EJBCA**, a separate section **Vendor specific details** is displayed after the CA Accounts section.The fields for Vendor specific details are as follows:

Vendor Specific Details for EJBCA CA - Field Description Table

Field	Description
***End Entity Profile Name**	Select a profile of an end entity.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the user name for the end entity.
***Issuer Common Name**	Select a common name of an issuer.
***Certificate Profile Name**	Select a profile name of certificate.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **Entrust** is selected as CA, The fields for Entrust CA are as follows:

Details for Entrust CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select a valid cert type associated with the CA account. If the **Certificate Category** radio button is selected to *Server*, the dropdown list is populated with the first available value. Select an appropriate value as required. If the **Certificate Category** radio button is selected to *Client*, the dropdown list is populated with 'None' as the default value.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

If the selected CA is Entrust, a separate section displaying **Vendor specific details** is displayed after the CA Accounts section.

Note: Based on the Entrust ECS account configuration **Custom Attributes section** may also be displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details for Entrust CA - Field Description Table

Field	Description
Additional Emails	Enter the valid email address in the field.
Requester Name	Enter the demo details
Requester Email	Enter a valid eamil id
Requester Phone	Enter the 10-digit phone number.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **Entrust MPKI** is selected as CA, the fields for Entrust MPKI CA are as follows:

Details for Entrust MPKI CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

If the selected CA is Entrust MPKI, a separate section **Vendor Specific Details** is displayed after the CA Accounts section. The following table provides the field description for Vendor specific details:

Vendor Specific Details for Entrust MPKI CA - Field Description Table

Field	Description
***CA Name**	Select a CA name from the dropdown list.
***Cert Profiles**	Select a cert profile from the dropdown list.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **GlobalSign** is selected as CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The fields for GlobalSign CA are as follows:

Details for GlobalSign CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Type**	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA, if the **Select CA =GlobalSign**, and the **Certificate type = Alpha SSL or Domain SSL**

Vendor Specific Details for GlobalSign CA - Field Description Table

Field	Description
***Domain Admin Email**	Select the email id to receive the approval requests from GlobalSign CA.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The following fields are displayed in the **Vendor Specific Details** section as per the selected CA, if the **Select CA =GlobalSign**, and the **Certificate type = Extended SSL**

Vendor Specific Details for GlobalSign CA - Field Description Table

Field	Description
***Incorporating Agency Reg. No**	Enter the Registration number of the incorporating agency.
***Designation**	Enter the designation of the requester.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Business Category**	Select the type of business (private org., government entity, or business entity

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The following field is displayed in the **Point of Contact** section as per the selected CA if the **Select CA =GlobalSign**, and the **Certificate type = Organization SSL** . The CA mandates the point of contact information (**First Name**) for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.

When **GlobalSign Atlas** is selected as CA

The fields for GlobalSign Atlas CA are as follows:

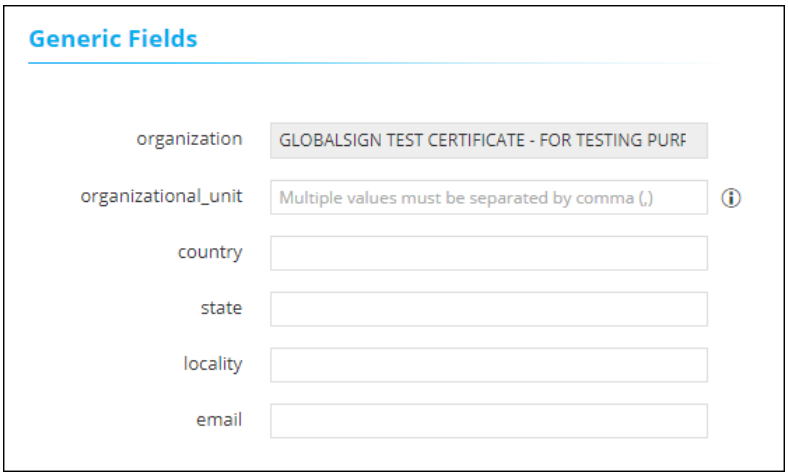
Details for GlobalSign Atlas CA - Field Description Table

Field	Description
***Select CA**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***API Credential Friendly name**	Select a CA Account to communicate with during the certificate enrollment actions.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Certificate**	Select the specific issuer certificate, that will be used for signing CSR by the certificate authority. Certs available in the root or intermediate cert inventory are displayed.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled. (in days/months/years)

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

A **Generic Fields** section is also displayed below the CA Accounts section. It contains the fields related to the CSR parameters based on the profile (API Credential Friendly name) selected. Only the Organization field is mandatory and is fetched from the selected profile. Rest of the fields are optional.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



When **GlobalSign MSSL** is selected as CA.

The fields for GlobalSign MSSL CA are as follows:

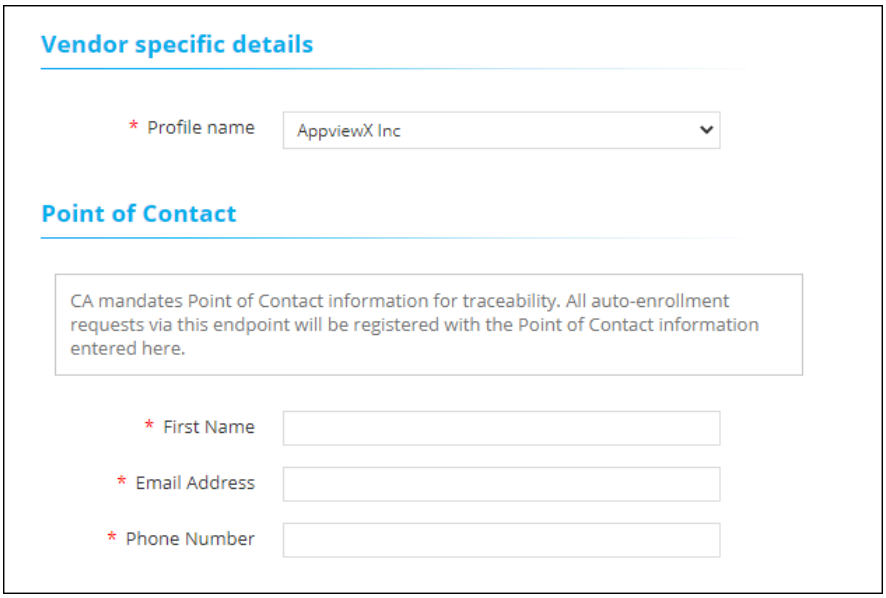
Details for GlobalSign MSSL CA - Field Description Table

Field	Description
CA Account	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
Product Type	Select the specific Certificate Type. The values are fetched from the CA Settings configuration.
CA Connector Name	Name of the CA connector after the certificate is enrolled.
Certificate Validity	Validity of the certificate to be enrolled. (in days/months/years)

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The following field is displayed in the **Vendor Specific Details** and **Point of Contact** section as per the selected CA:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Vendor Specific Details for GlobalSign MSSL CA - Field Description Table

Field	Description
***Profile**	Select the Profile based on the configurations made in the Certificate Authority setting.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The following field is displayed in the **Point of Contact** section as per the selected CA. The CA mandates the point of contact information for traceability. All auto-enrollment requests via this endpoint are registered with the point of contact information entered here.

Point of Contact Details for GlobalSign MSSL CA - Field Description Table

Field	Description
***First Name**	Enter the first name.
***Email Address**	Enter the valid email address.
***Phone Number**	Enter the valid phone number.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

When **Google** is selected as CA, the fields for Google CA are as follows:

Details for Google CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Type 3 or more letters of the certificate keywords after which a list of server certificates issued from the above selected CA account will be displayed, one certificate can be selected for further communications with CMP client machine.
***Issuer Location**	Select the issuer location associated with the CA account.
***Issuer Name**	Select a issuer name to issue the certificate.
Template Name	Select a template name from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The fields for Vendor Specific details are as follows:

Field	Description
Certificate ID	Enter the valid certificate id.

When **HydrantID** is selected as CA, the fields for HydrantID CA are as follows:

Details for Lets HydrantID CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***HydrantID Policy**	Select the policy associated with the CA Account to be used for certificate operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **IDnomic** is selected as CA, the fields for IDnomic CA are as follows:

Details for IDnomic CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Profile**	Select the certificate Profile from the dropdown list.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **Microsoft Enterprise** is selected as CA, the fields for Microsoft Enterprise CA are as follows:

Details for Microsoft Enterprise CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

If the selected CA is Microsoft Enterprise, a separate section displaying **Vendor specific details** is displayed after the CA Accounts section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Field	Description
***Template Name**	Select the desired template name. This value is based on the policy setting and its group association.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **Microsoft Standalone** is selected as CA, the fields for Microsoft Standalone CA are as follows:

Details for Microsoft Standalone CA - Field Description Table

Field	Description
***CA Account**	Select the specific CA Account associated with the selected CA to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **Nexus** is selected as CA.

The fields for Nexus CA are as follows:

Details for Nexus CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled (in days/months/years).

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

The following field is displayed in the **Vendor Specific Details** section as per the selected CA:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Field	Description
***Procedure**	Select the Procedure based on the configurations made in the Certificate Authority Setting.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **OpenTrust** is selected as CA.

The fields for OpenTrust CA are as follows:

Details for OpenTrust CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA which is to be used for certificate creation operations.
***Certificate Management Profile**	Select one issuer certificate from the dropdown list. This issuer certificate will be used for signing the CSR by the certificate authority. **Note:** Only the issuer certificates available in the root or intermediate certificates inventory will be shown for selection.
Zone	Select the zone pertaining to the Certificate Management Profile
***CA Connector Name**	Name of the CA connector after the certificate is enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

When **Sectigo (Comodo Certificate Manager)** is selected as CA. The fields for Sectigo (Comodo Certificate Manager) CA are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for Sectigo (Comodo Certificate Manager) CA - Field Description Table

Fields	Description
***CA Account**	A unique name to identify the CA setting. **Note**: No special characters other than '.', '-','_' are allowed. Names should not start with special characters.
***Purpose/Usage**	Certificate Type for which CLM actions will be enabled. *Example*: Server and Client.
Proxy Required	Enable this field if the CA communication needs to happen via Proxy. The proxy details configured in general settings will be used for communication.
Data Center (AppViewX's CA agent)	Select the data center through which the CA communication needs to happen. (CC node is recommended) i.e., whichever node is selected the communication will happen via that CC node.
CA Configuration	
***Base URL**	This URL will contain the hostname of the Sectigo CA instance and used for constructing the API requests.
***Login URI**	Provide the customer login URI for API authentication.
***User Name**	Enter the Username of the Sectigo portal to communicate with the CA.
***Password**	Enter the Password of the Sectigo portal to communicate with the CA.
***Organization Id**	Enter the organization id used for the certificate lifecycle action. (You will find it in the Organization tab of the Sectigo portal)
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.	

When **SwissSign** is selected as CA, the fields for SwissSign CA are as follows:

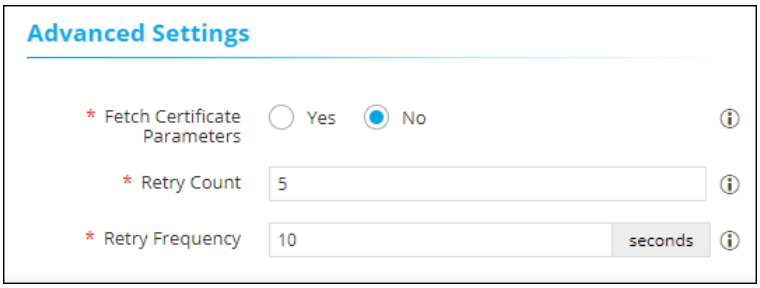
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Details for SwissSign CA - Field Description Table

Field	Description
***CA Account**	Select a specific CA Account from the selected CA to be used for certificate creation operations.
***Client Name**	Select the specific client.
***Product**	Select the specific product.
***Server Certificate**	Select the certificate issued by the selected CA using which the trusted inventory is validated. You can search for it by typing the exact common name or the serial number.
***CA Connector Name**	Name of the CA connector after the certificate is being enrolled.
***Certificate Validity**	Validity of the certificate to be enrolled.

Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

6. Configure the **Advanced Settings** section as follows:



The following table provides the field description for the Advanced Settings section:

Advanced Settings - Field Description Table

Field	Description
***Fetch Certificate Parameters**	Setting the radio button to Yes, will enable the system to automatically fetch certificate parameters from a Suggestive Policy, and append them to the client CSRs.
***Retry Count**	Specify a retry count up to which the agent will retry for the certificate to be fetched.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Retry Frequency**	Specify a retry frequency up to which the agent will wait for each retry count.

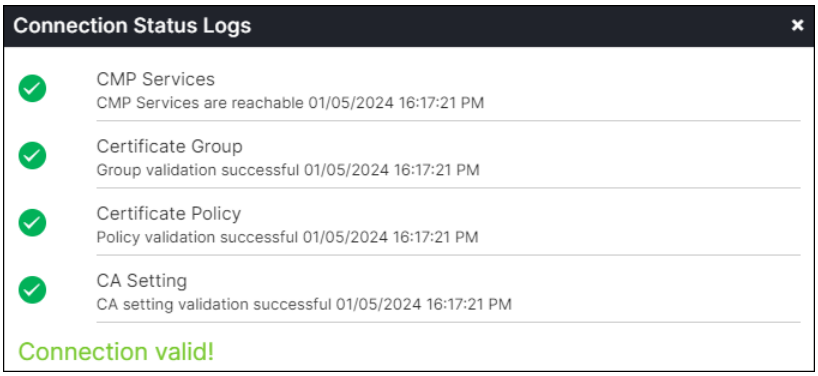
Note: Fields with the red asterisk (*) symbol indicate mandatory fields.

Validating CMP

Once the CMP settings are added validation needs to be done to check whether the CA and Agent related details are properly configured.

1. Go to **(Menu)** > **CERT+** > **Administration** > **Auto Enrollment** > **SCEP**.
2. On the **CMP** page, click **Check** from the Status column to validate the CMP setting that has been created.
   The CMP settings will be validated and the **Status** will be shown as either **Success** or **Failure**.

   Success Scenario



WAEP

Windows Auto-Enrollment Proxy (WAEP) is a powerful component developed by AppViewX to enable seamless certificate enrollment and migration for users and devices within a Microsoft domain. Designed to automate and simplify certificate lifecycle management, WAEP allows organizations to transition from their existing certificates to AppViewX PKI (Public Key Infrastructure).

WAEP comes equipped with extensible features that enhance its functionality and adaptability to enterprise needs. It includes the ability to automatically fetch certificate templates, streamlining the configuration process by dynamically pulling template details from the Microsoft Certificate Authority

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

(CA). Additionally, WAEP supports per-template CA configuration, allowing administrators to specify distinct types of certificate for different templates, thereby offering greater control and flexibility. This robust integration empowers organizations to leverage their existing Microsoft domain infrastructure while benefiting from the advanced capabilities of AppViewX PKI.

Key Reasons to Migrate to PKI with WAEP

Migrating to AppViewX PKI using WAEP provides organizations with a modern, centralized approach to certificate lifecycle management, offering significant advantages over traditional Microsoft Certificate Authority (MSCA) solutions. While MSCA serves basic certificate needs within a Microsoft domain, it often falls short in providing unified visibility and efficient management of certificates across diverse environments. AppViewX PKI addresses these challenges by offering a single point of management for all certificates, enabling better control, enhanced visibility. This migration eliminates the complexity of managing certificates in fragmented systems, ensuring seamless integration.

AppViewX PKI includes advanced features such as centralized reporting, real-time certificate monitoring, and streamlined template configuration using WAEP. These capabilities allow organizations to maintain compliance, reduce operational inefficiencies, and strengthen their overall security posture, making it a superior choice for enterprises looking to upgrade from MSCA.

Microsoft CA Native Data Flow: Pre-AppViewX Stage

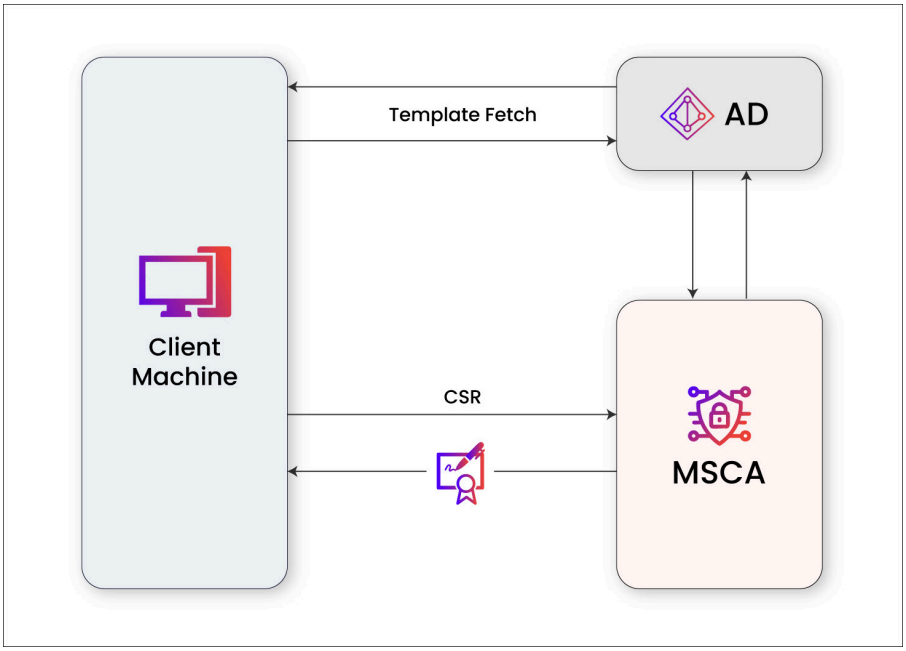
MSCA auto-enrollment can be configured in two ways:

- MSCA is installed without the Certificate Enrollment Policy (CEP) and Certificate Enrollment Services (CES) components
- MSCA is installed with the CEP and CES components

Both scenarios are explained as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. **MSCA Auto-Enrollment without CEP and CES**



Template Retrieval

The client machine sends a request to fetch the templates configured in the Active Directory (AD), and these templates are used for certificate enrollment.

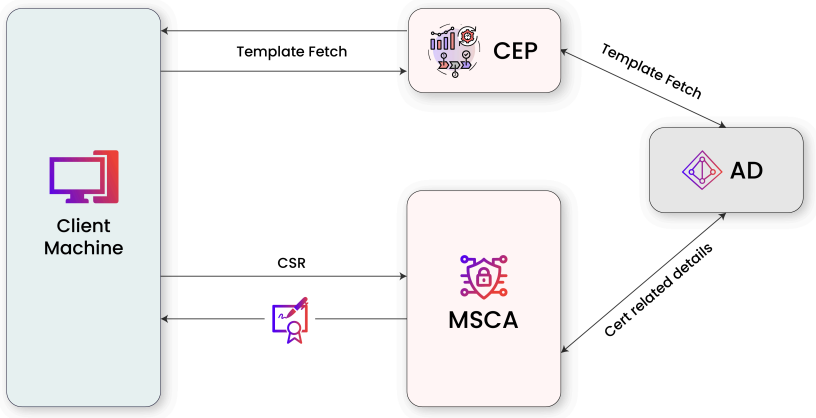
Certificate Enrollment Request and issuance

The client machine initiates a certificate enrollment call with a CSR to the MSCA and the MSCA issues the certificate to the end machine. If this is the existing environment, then CEP and CES must be installed and configured as mentioned in the Section, Prerequisites to proceed with WAEP.

2. **MSCA Auto-Enrollment with CEP and CES**

The following diagram illustrates the flow of the MSCA certificate enrollment process, starting from the Windows machine requesting a certificate to the issuance under the same domain.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Template Retrieval

The client machine sends a request to fetch the templates configured in the CEP, and these templates are used for certificate enrollment.

Certificate Enrollment Request and issuance

The client machine initiates a certificate enrollment call with a CSR to the MSCA and the MSCA issues the certificate to the end machine.

AppViewX-WAEP: Understanding the Data Flow

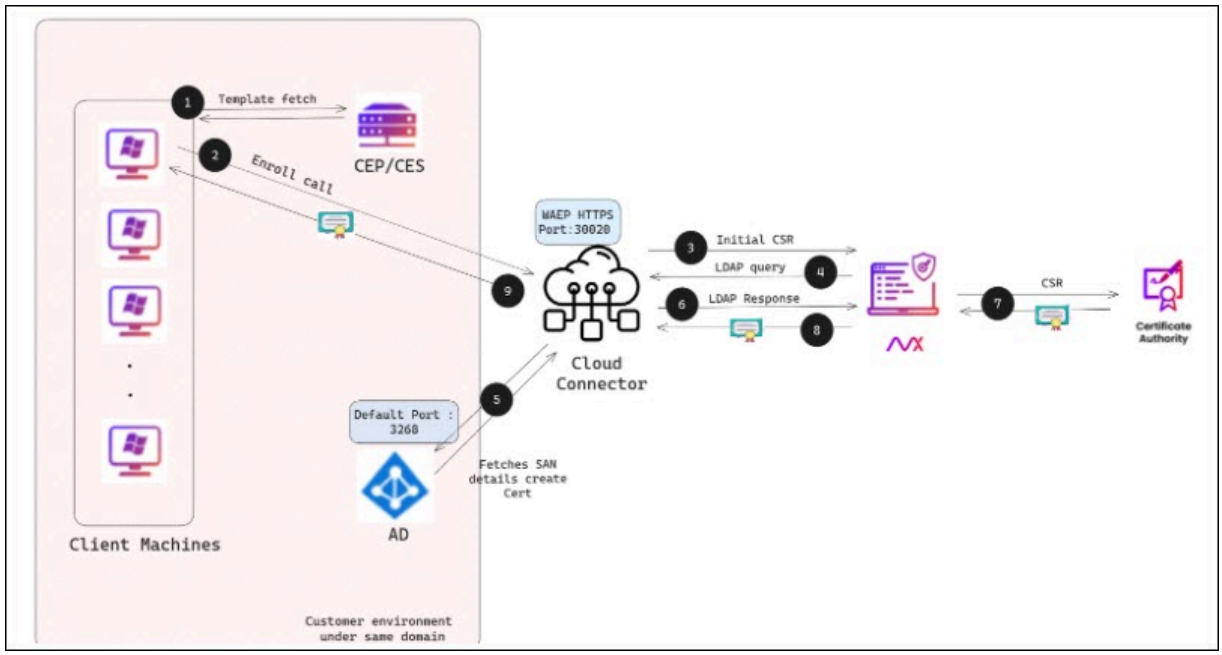
AppViewX auto-enrollment is supported through two approaches:

1. **CEP/CES**

   The following diagram illustrates the entire flow of the WAEP certificate enrollment process THOUGH cep/ces , starting from the Windows machine requesting a certificate to the PKI+ issuance of the certificate.

   The following diagram illustrates the entire flow of the WAEP certificate enrollment process, starting from the Windows machine requesting a certificate to the PKI+ issuance of the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Explanation of each call and its corresponding number is detailed:

- **Template Retrieval [1-2]**

  The client machine sends a request to fetch the templates configured in the CEP. CEP fetches the template from AD and responds to the request

- **Certificate Enrollment Request [3-4]**

  The client machine initiates a certificate enrollment call with a CSR to the cloud connector (CC) machine for a selected template. And the initial CSR is forwarded to AppViewX.

- **LDAP Query for SAN Details [5-7]**

  An LDAP query is made to retrieve SAN details from the AD machine via the cloud connector from AppViewX.

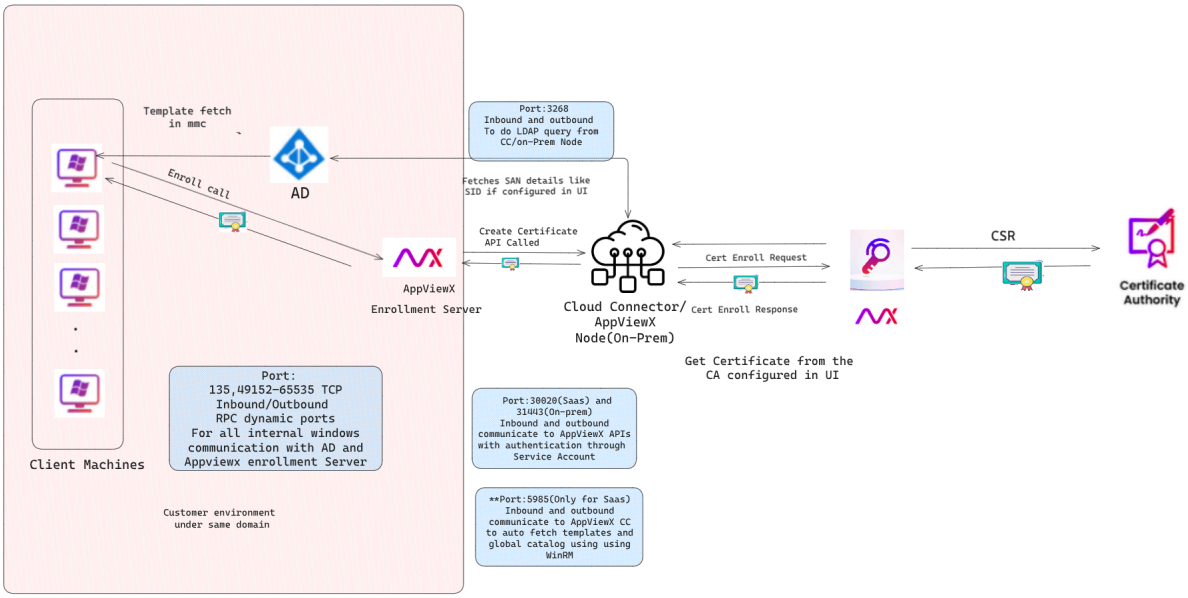
- **Certificate Issuance [8-10]**

  The SAN details are added to the certificate request, and the CSR is submitted to the CA for issuance. The issued certificate is then returned to the client machine.

2. **AppViewX Auto-enrollment Server**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

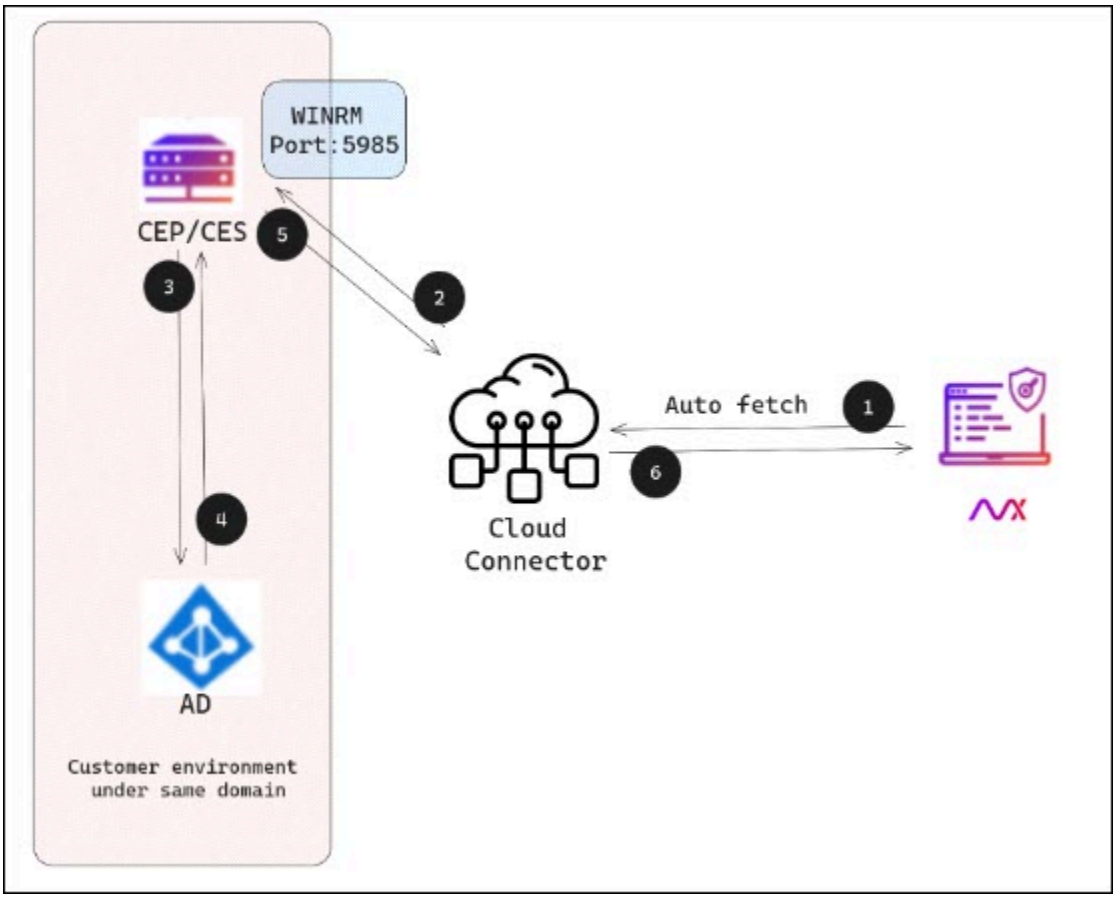
The following diagram illustrates the entire flow of the WAEP certificate enrollment process through AppViewX Enrollment Server starting from the Windows machine requesting a certificate to the PKI+ issuance of the certificate.



Auto-Fetch of Templates and Global Catalog (Applicable only for SaaS)

An auto-fetch call is initiated by AppViewX to the CC. Using WinRM, the query is executed on the CEP/ AppViewX Enrollment Server, which in turn retrieves the details from the AD machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



The diagram explains the flow of auto-fetch of templates:

- AppViewX sends an auto-fetch request to the cloud connector (CC).
- The CC uses the WinRM to execute a query on the CEP/AppViewX Enrollment Server machine.
- The CEP/AppViewX Enrollment Server machine retrieves the certificate details from the Active Directory (AD).
- The fetched data is sent back to AppViewX for processing.

- CEP/CES
- AppViewX Enrollment Server
- Troubleshooting

CEP/CES

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Prerequisites
• Configuration Steps
• AppViewX WAEP Configuration

Prerequisites

Key Requirements

- **Service Account Configuration:** Ensure the service account is correctly set up with the necessary permissions.
- **CEP and CES Services:** Verify that Certificate Enrollment Policy (CEP) and Certificate Enrollment Services (CES) are installed and configured within the domain.

Configuration Steps

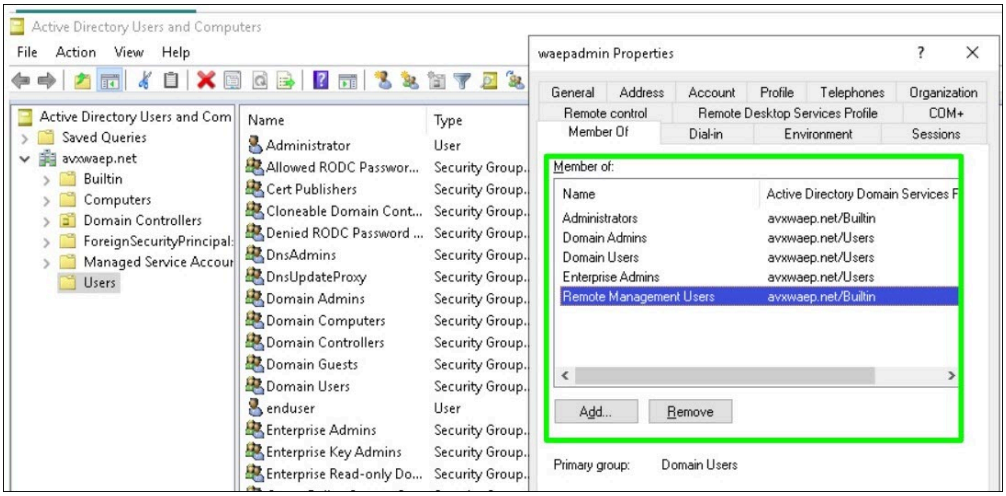
If CEP and CES are already installed and configured, you can proceed directly with the AppViewX WAEP Configuration. Ensure the prerequisites are verified to avoid any interruptions during the setup process.

• Configurations in AD
• Configurations in CEP/CES machine
• Updating CEP URL in AD
• Adding Templates in CA
• Validating MSCA using CEP/CES in Client Machine

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configurations in AD

1. Create a service account from the user group in the AD machine with the following permissions as shown:



2. Set the delegations in the AD machine using the following commands:

   a. `Get-ADUser -Identity <service_account> | Set-ADAccountControl -TrustedToAuthForDelegation $True`

   b. `Set-ADUser -Identity <service_account> -Add @{'msDS-AllowedToDelegateTo'=@('HOST/<CEP_machine_FQDN>','RPCSS/<CEP_machine_FQDN>')}`

Configurations in CEP/CES machine

1. **CEP/CES Installation**

   To install the Certificate Enrollment Services on the CEP/CES server:

   a. Open the Server Manager.
   b. Click **Add Roles and Features,** and click **Next**.
   c. Select Role-based or feature-based installation, and click **Next**.
   d. Choose **Select a server from the server pool,** and click **Next**.
   e. Expand the **Active Directory Certificate Services**, select **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service,** and click **Next**.
   f. Proceed until the **Confirmation** page, and click **Install**.

2. **CEP/CES Configuration**
   a. Click the new task shown in the **Server Manager notifications: Configure Active Directory Certificate Services** on the destination server.
   b. In the credentials panel shown, click **Change**.
   c. Enter an account service account which we created, click **OK** and then click **Next**.

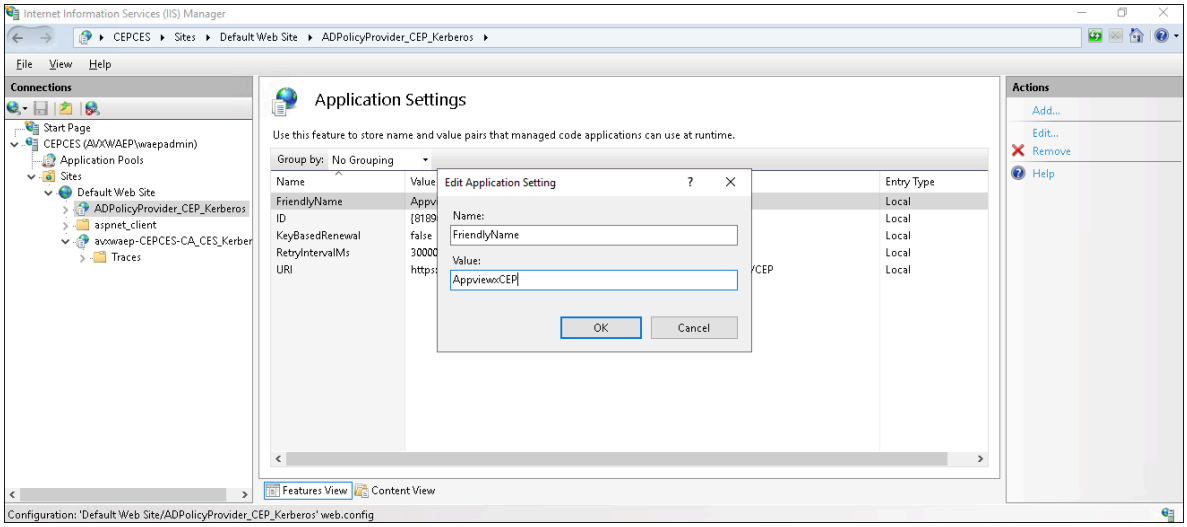
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

d. Select **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service** and click **Next**.
e. Select the CA Name.
f. Click **Select** and choose the Microsoft CA that will be issuing the certificates using certificate enrollment web service, click **OK** and then click **Next**.
g. For CES authentication type, select **Windows Integrated Authentication** and then click **Next**.
h. For CES service account, select **use built in application pool identity.**
i. Click **OK** and then click **Next**.
j. For CEP authentication type, select **Windows Integrated Authentication** and then click **Next**.
k. For Certificate authentication, select **Choose and assign a certificate for SSL later** and click **Next**.
l. Review the confirmation page and click **Configure**.
m. When the installation completes, click **Close**.

3. **Configuring IIS in CEP/CES machine**

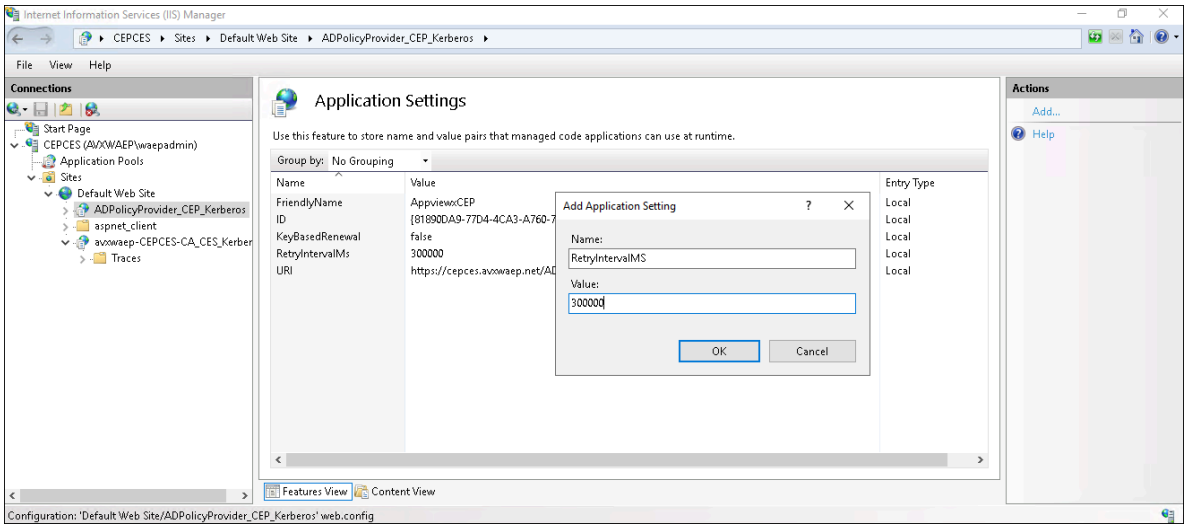
To configure the Internet Information Services (IIS) on ADCS:

a. Type InetMgr.exe in the command prompt to open the Internet Information Services (IIS) Manager.
b. Click your server name on the left-hand side.
c. Expand the selection for your server and click **Application Pools**.
d. Expand the default web site and click **ADPolicyProvider_CEP_Kerberos** and open **Application Settings**.
e. Edit the entry name **FriendlyName** and set the value to **AppViewX_Enrollment.** This is a name that clients will see only when they are manually requesting for certificates.



f. Click **Add** and create a new entry with the name **RetryIntervalMs** and value **300000**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

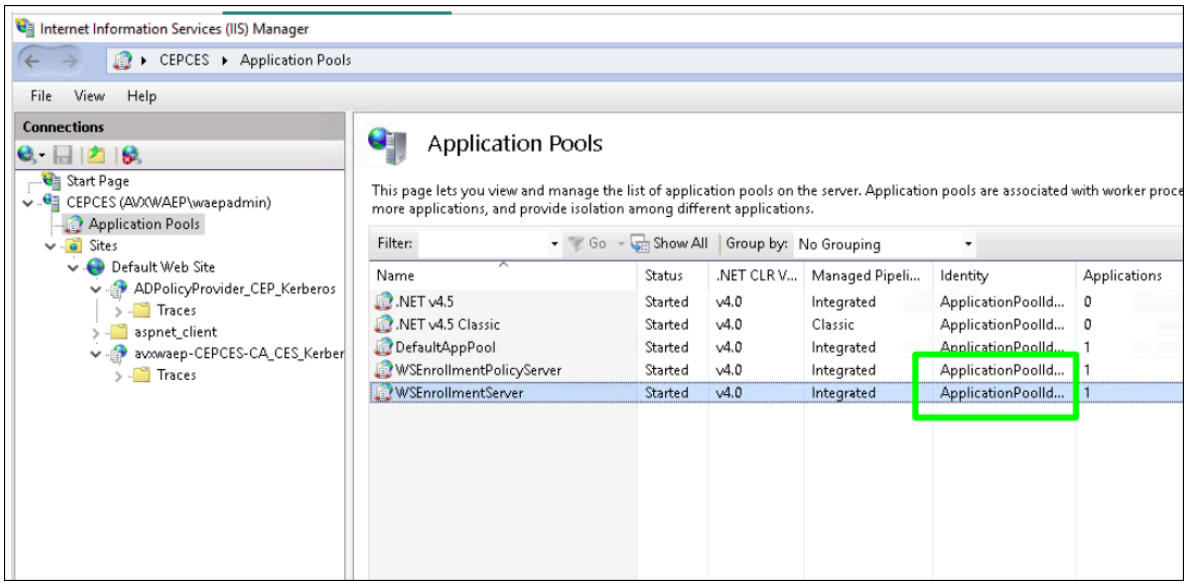


g. Click the URI and copy the URI to use for group policy updates.

h. Restart IIS by clicking the server name and then click **Restart** on the right-hand side.

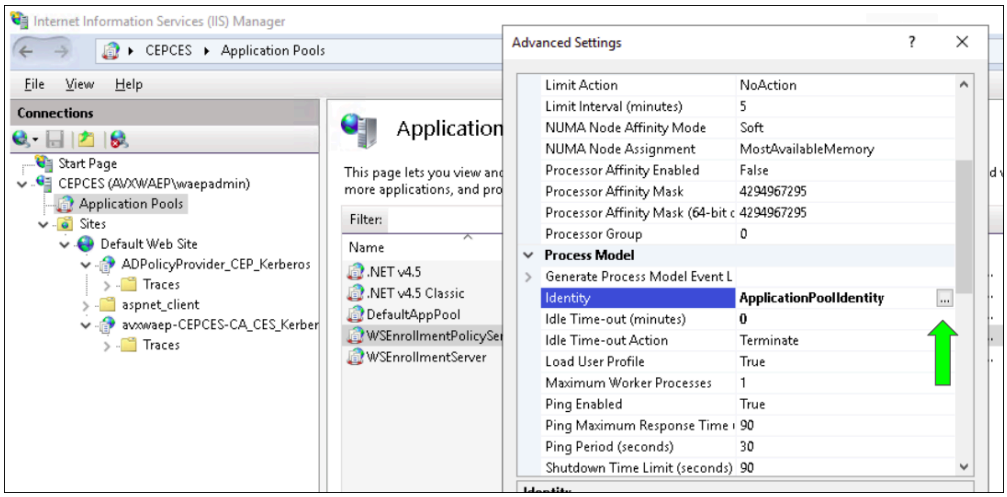
4. **Steps for configuration verification**

a. Validate if **Identity of WSEnrollmentPolicyServer** and **WSEnrollmentServer** is set to **ApplicationPoolsIdentity**.

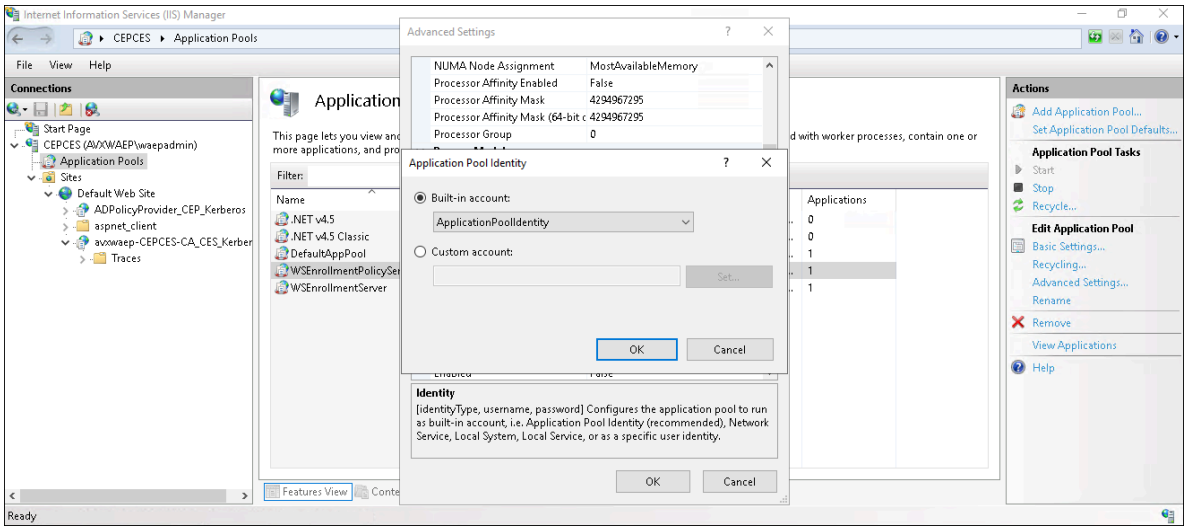


If not, right-click the application pool name and click **Advanced Settings > Identity**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



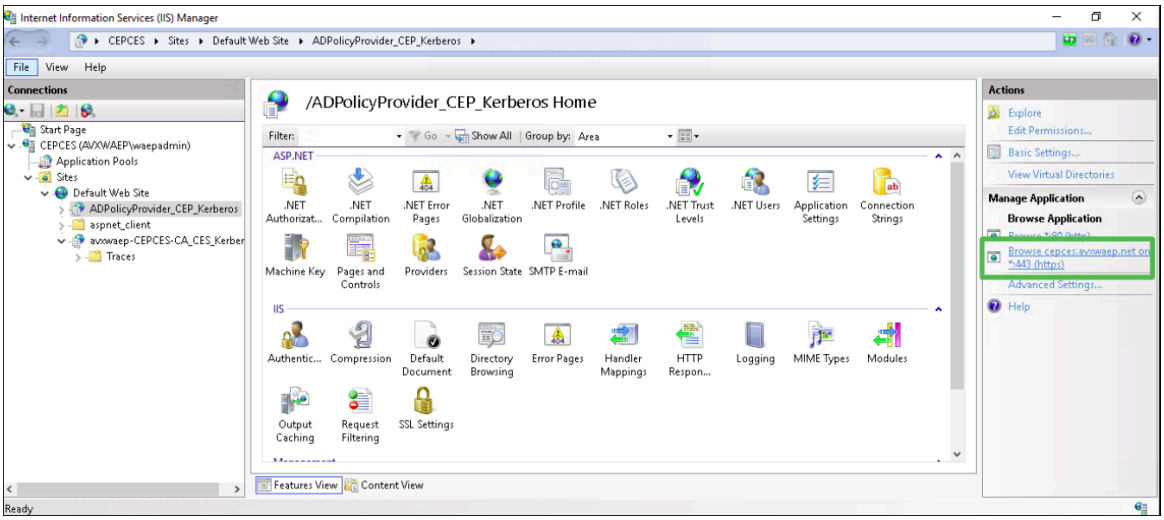
Click the three dots at the end of the identity and configure it as **Built in account > ApplicationPoolIdentity** as shown:



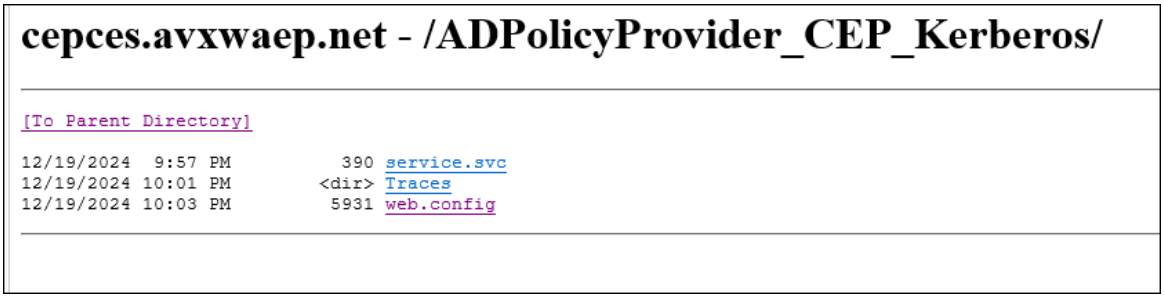
b. Enable directory browsing for validation.

- By clicking the website name **[ADPolicyProvider_CEP_Kerberos] > Directory browsing > Enable [Right Pane]**
- Once enabled, click the **Browse Application** URL as shown, and enter the service account credentials if required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



The expected output is as shown:

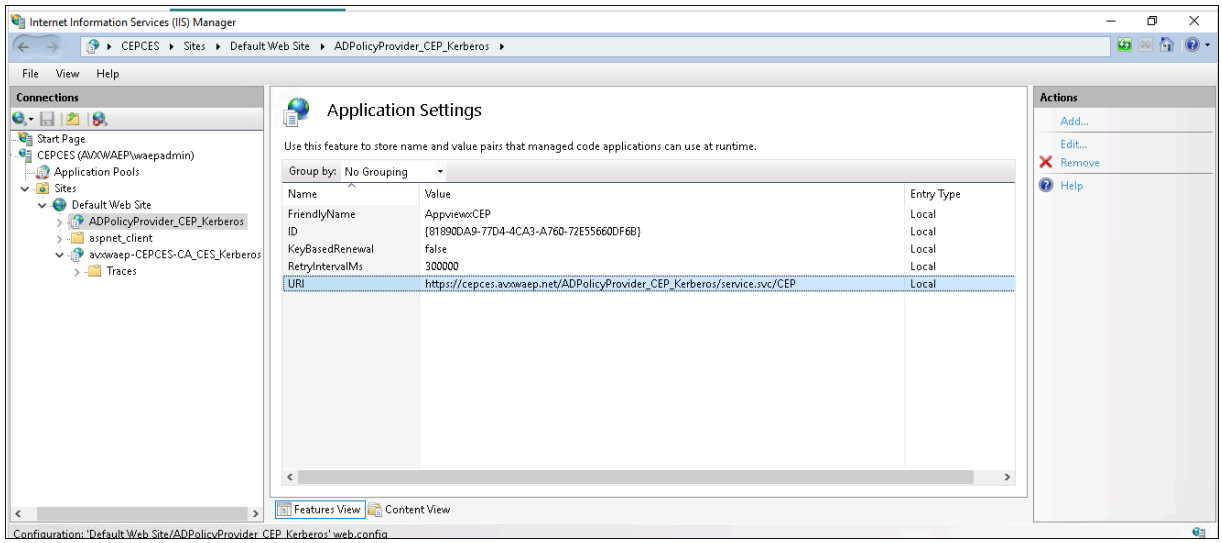


- Similarly enable the directory browsing and verify browsing for the CES [<CA_NAME>_CES_Kerberos].

Updating CEP URL in AD

1. Login to an AD machine using the service account created.
2. Get the CEP URL from the CEP/CES machine by going to **IIS > ADPolicyProvider_CEP_Kerberos > Application settings > URL**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



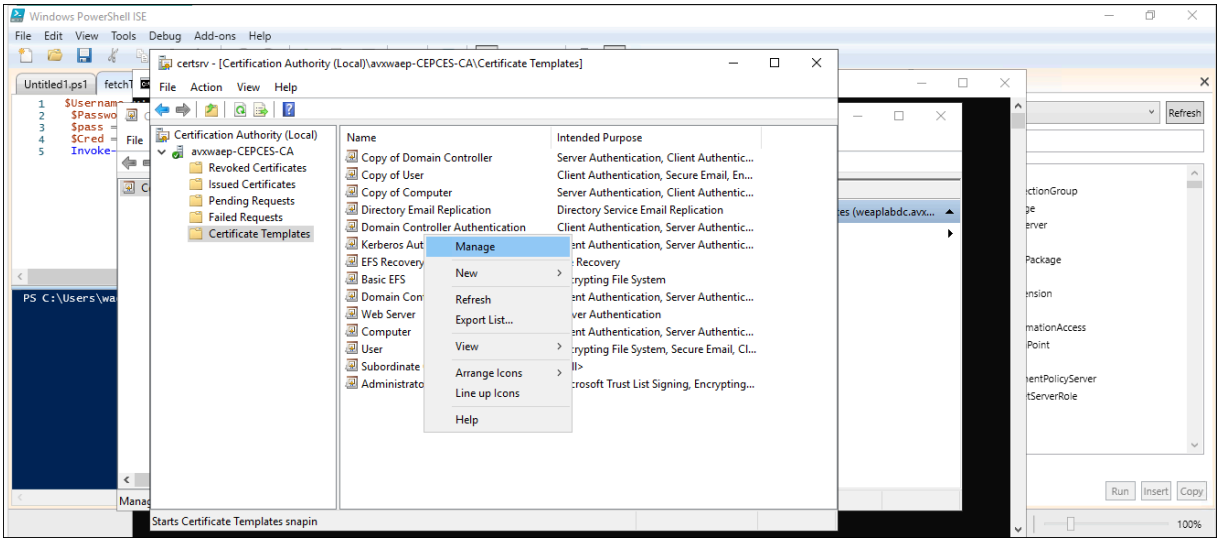
3. To update the Group Policy for Certificate Enrollment:
   a. Type `gpmc.msc` in the **Run** command to access Group Policy Management on the AD Domain Services server.
   b. Expand your domain forest > Domains > your domain name, and then select **Default Domain Policy.**
   c. Right-click **Default Domain Policy** and select **Edit**.
   d. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.**
   e. Edit **Certificate Services Client – Certificate Enrollment Policy.**
   f. Change **Configuration Model** to *Enabled*.
   g. Remove the **Active Directory Enrollment Policy** from the Certificate Enrollment policy list, and click **Add.**
   h. Enter the policy server URI copied from the previous step, click Validate Server, and click **Add.**
   i. Select **Default**, and click **Add.**
   j. Expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.**
   k. Edit **Certificate Services Client – Certificate Enrollment Policy.**
   l. Change **Configuration Model** to *Enabled*.
   m. Remove the **Active Directory Enrollment Policy** from the Certificate Enrollment policy list, and click **Add.**
   n. Enter the policy server URI copied from the previous step, click **Validate Server,** and click **Add.**
   o. Select **Default,** and click **OK.**
4. Open the command prompt as administrator and run the gpupdate /force command to update the group policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

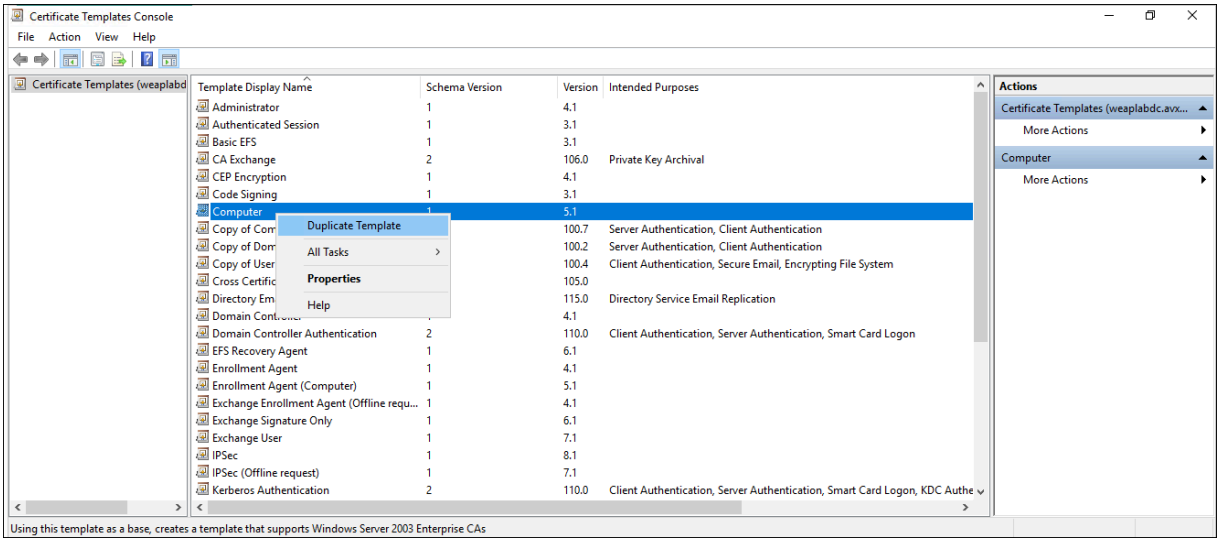
Adding Templates in CA

To ensure proper functionality with WAEP, the default templates must be duplicated. Follow these steps to duplicate the templates on the CEP/CES machine:

1. Open the **Run** dialog and enter certsrv.msc to launch the Certificate Authority interface.
2. Select the MSCA in use, then click on **Templates**.
3. On the right pane, right-click and select **Manage**.

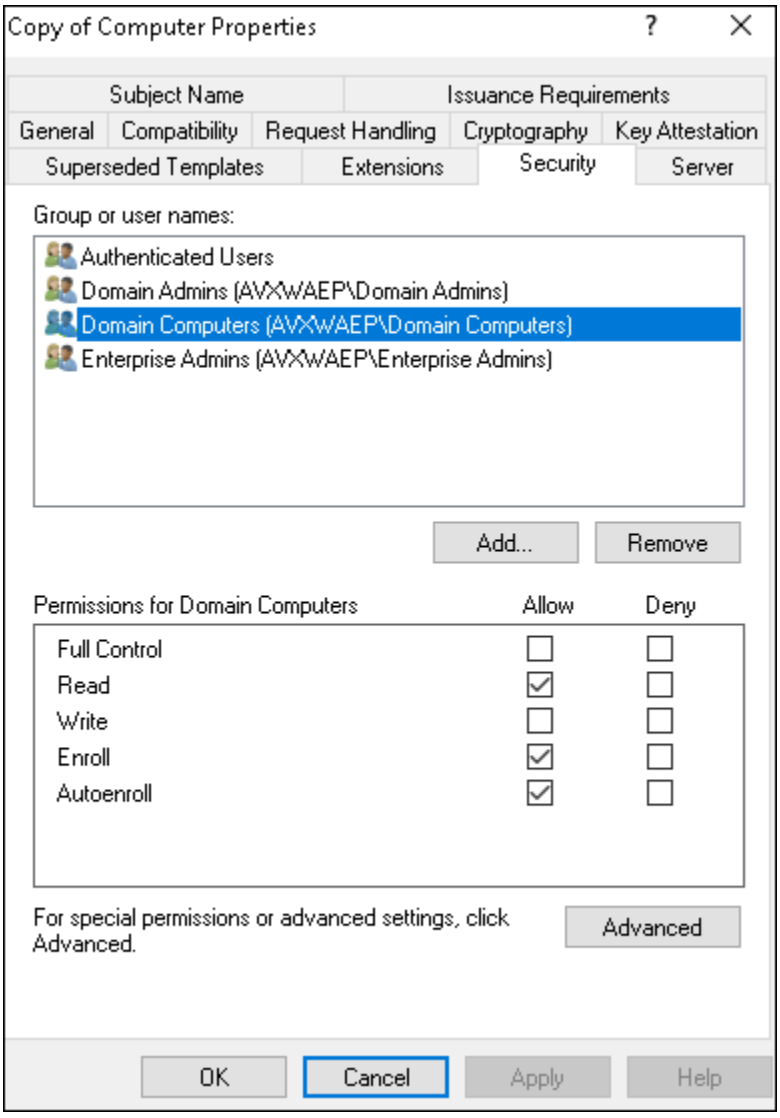


4. Locate the **Computer** template, right-click and choose **Duplicate Template**. Click **OK** to confirm.



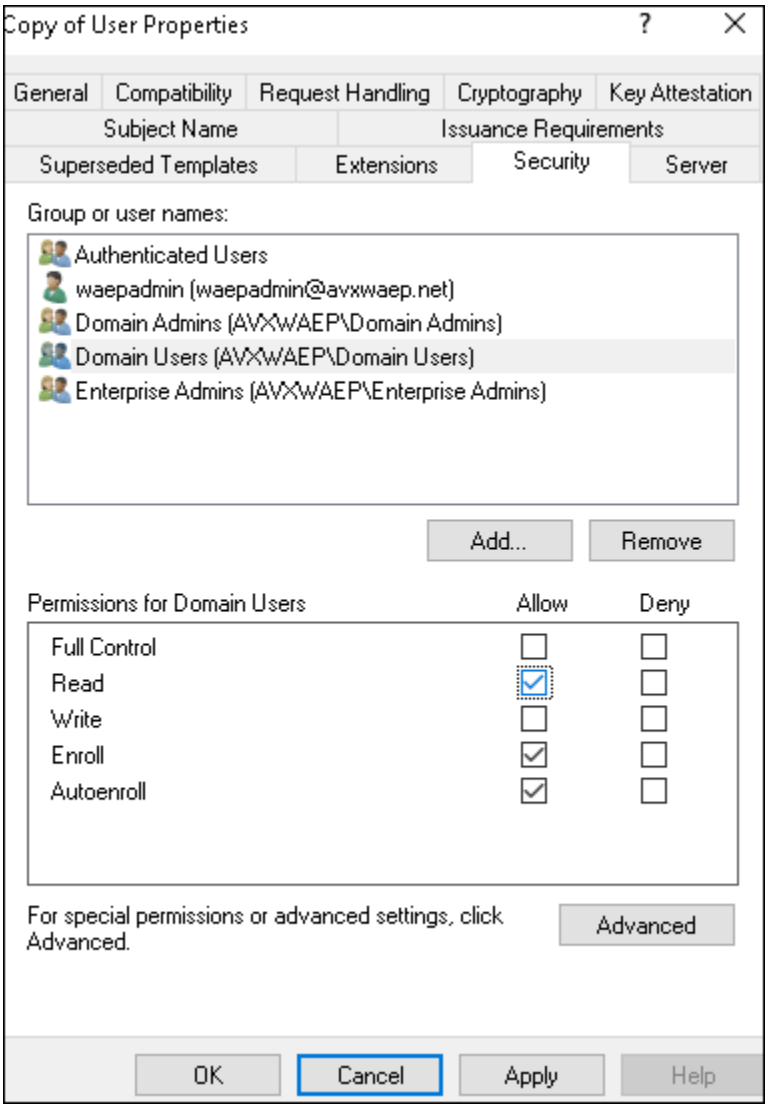
5. Ensure that the following permission for the domain computer is provided for the computer template:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

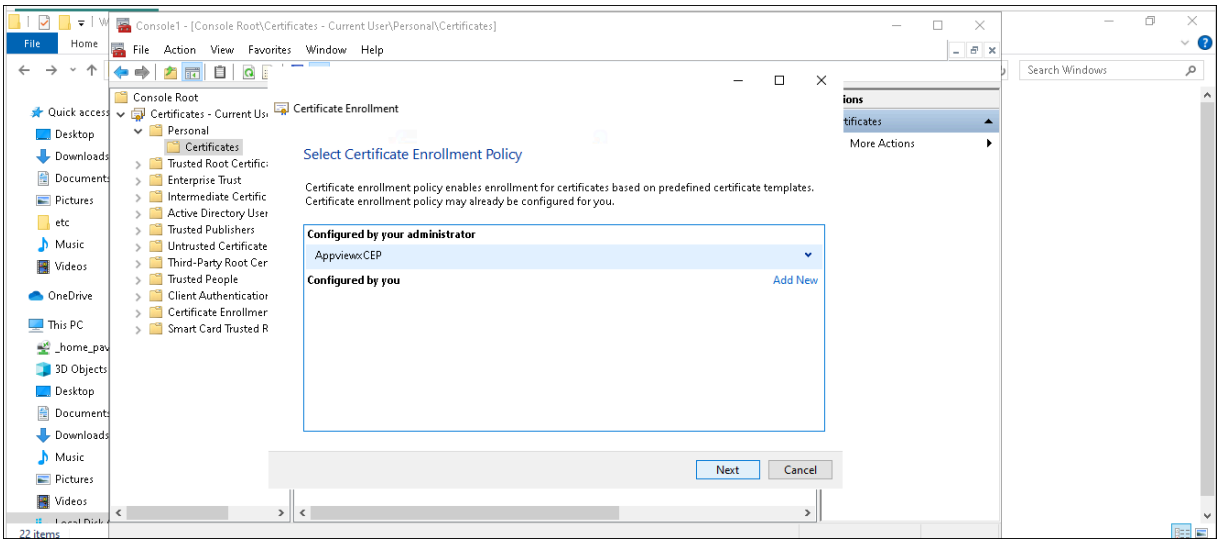
6. Repeat the process to duplicate the **User** template as well with permission for the domain users as shown:



Validating MSCA using CEP/CES in Client Machine

1. Login to an end machine using the service account created.
2. Open a command prompt as administrator and run the gpupdate /force command to update the group policy.
3. Go to MMC and add the user and machine certificate snap-ons.
4. Right-click the personal store of User Certificates and click **All-tasks > Request New Certificate.** The CEP friendly name configured earlier will be shown there. Click that and proceed to enroll a certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. Similarly test certificate enrollment for computer certificates.

AppViewX WAEP Configuration

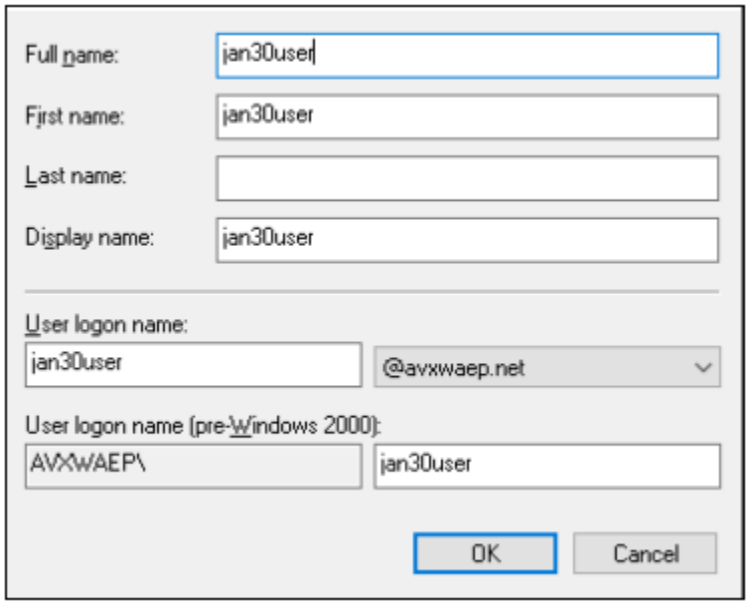
- System Requirements and Service Account Configuration
- Configuring WAEP Templates
- Configuring Windows Auto-Enrollment Proxy

System Requirements and Service Account Configuration

1. **A valid Service Account with the below permissions**
   - Enterprise Admin
   - Domain Admin
   - Remote Management Users
   - Administrator
   - Domain User
2. **Service account name**

   Ensure that the service account's full name is the same as the login name as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



3. **CC Service Setup**
   - Install ACME-HTTPS and SCEP-HTTP services on the CC.
   - Configure WAEP in the AppViewX GUI specific to CC.
4. **Domain Machine Requirements**
   - **SaaS Setup**
     - **Outbound Calls**
       - Port 30020 for unidirectional communication from domain machines to CC.
       - Port 30022 for CRL verification.
     - **Inbound Calls**
       - Port 5985 for auto-fetch requests from CC to the CEP machine.
   - **On-prem Setup**
     - **Outbound Calls**
       - Port 31443 for unidirectional communication from domain machines to CC.
       - Port 30022 for CRL verification.

> **Note:** Auto fetch/lift and shift functionalities are only supported in the SaaS model.

5. **Domain and Connectivity**
   - CEP must be in the same domain as the AD, with connectivity to the AD server.
   - Ensure a valid DNS record for the CC/AppViewX node exists in domain machines.
6. **Certificate and Trust Configuration**
   - Issue the certificate using AppViewX PKIaaS CA and enable trust on Windows domain machines.
   - Steps to add root and intermediate certificates to the Windows domain machines:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Log onto the AD machine using your service account.
b. Move the root and intermediate certificates that need to be trusted to the appropriate location.
c. Open the command prompt with administrator privileges.
d. To publish the **Issuing CA** certificate, run:

```
certutil -dspublish -f <PathToCertFile.cer> SubCA
```

e. To publish the **Root CA** certificate, run:

```
certutil -dspublish -f <PathToCertFile.cer> RootCA
```

f. Run the following command to force a policy update and push the certificates to the domain machines:

```
gpupdate /force
```

Configuring WAEP Templates

Templates can be fetched in two ways: manual and automatic. Fetching templates is essential for mapping each template to a specific CA configuration setting.

Note: To ensure proper functionality with WAEP, default templates must be duplicated. Follow these steps to duplicate templates on the CEP/CES machine from the Section, Adding Templates in CA.

Manual Fetch Configuration

Prerequisites

- Generate CSV file (Applicable only for manual upload of templates)

To generate CSV file:

1. Run Windows PowerShell.
2. To extract information of the certificate name, certificate template OID, validity period, and renewal period from the templates published on the ADCS server, run the command on the ADCS server:

```
Certutil -adtemplate -v | select-string distinguishedName,msPKI-Cert-Template-OID,pKIExpirationPeriod,pKIOverlapPeriod,'Major Version Number','Minor Version Number'
```

3. Copy the distinguished name (Template name), certificate template OID, validity period, and renewal period with major and minor version for templates as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
distinguishedName = Copy of Computer
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.60046.11887992.1200005.2037137.6303374.216.548621.13969983 Copy of
mputer
pKIExpirationPeriod =  4 Years
pKIOverlapPeriod =  6 Weeks
      Major Version Number=100
      Minor Version Number=42
distinguishedName = Copy of User
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.60046.11887992.1200005.2037137.6303374.216.9121815.3879205 Copy of
er
pKIExpirationPeriod =  2 Years
pKIOverlapPeriod =  16 Weeks
      Major Version Number=100
      Minor Version Number=16
distinguishedName = Copy of Domain Controller
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.60046.11887992.1200005.2037137.6303374.216.16363737.13866587 Copy of
main Controller
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
      Major Version Number=100
      Minor Version Number=2
distinguishedName = copy_of_Copy of Computer
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.60046.11887992.1200005.2037137.6303374.216.548621.13969984
pKIExpirationPeriod =  1 Years
pKIOverlapPeriod =  6 Weeks
      Major Version Number=100
      Minor Version Number=11
distinguishedName = Citrix_RegistrationAuthority_ManualAuthorization
msPKI-Cert-Template-OID = 1.3.6.1.4.1.311.21.8.60046.11887992.1200005.2037137.6303374.216.14427574.9208993
itrix_RegistrationAuthority_ManualAuthorization
pKIExpirationPeriod =  1 Days
pKIOverlapPeriod =  EMPTY
      Major Version Number=2
      Minor Version Number=0
```

4. Open a spreadsheet and create column headings:
   - **templateName:** In this column, add entries as Computer_Auto_enrollment template and User_autoenrollment.
   - **templateOID:** In this column, paste the OIDs copied in Step 3 against the respective template.
   - **validityPeriod:** In this column, enter the value as 365, which is the default value of the validity period.
   - **validityPeriodUnit:** In this column, enter the value as *days, weeks, months, or years*.
   - **renewalPeriod:** In this column, enter the value as 30, which is the default value of the renewal period.

     Note: The renewal period must be less than the validity period.

   - **renewalPeriodUnit:** In this column, enter the value as *hours, days, weeks, months, or years*.
   - **templateMinorVersion:** In this column, please enter the minor version associated with the template.
   - **templateMajorVersion:** In this column, please enter the major version associated with the template.
5. Once done, save the file in .xls, or .xlsx, or csv format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Auto-Fetch Configuration

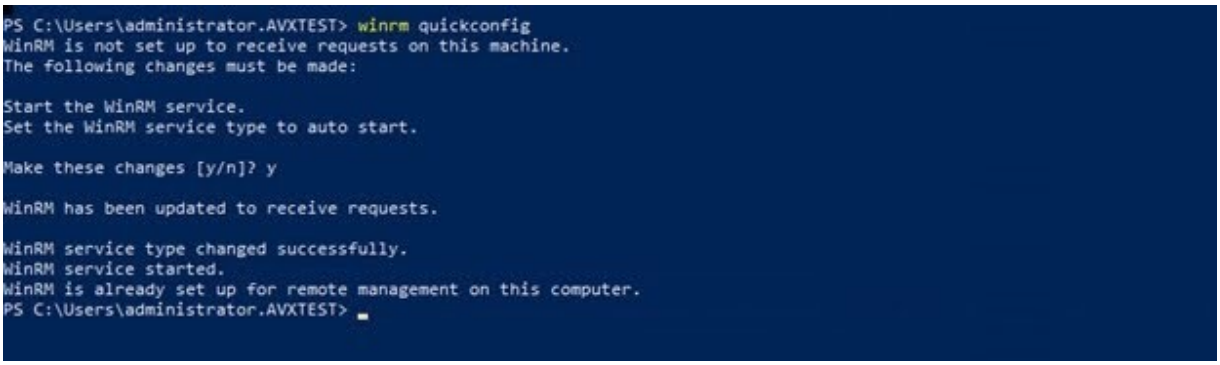
Templates can also be automatically fetched from the Windows machines using WAEP. To use auto-fetch:

Enable Winrm services in AD and CEP machine

For the Lift & Shift feature to work, enable the WinRM service on the policy server (CEP/CES) and the AD servers configured in WAEP for global fetch configuration and publication of templates.

To configure WinRM service (Applicable only for automatic upload of templates):

1. Run winrm quickconfig on the PowerShell window as an administrator.
2. Type *y* when prompted to start the WinRM service.



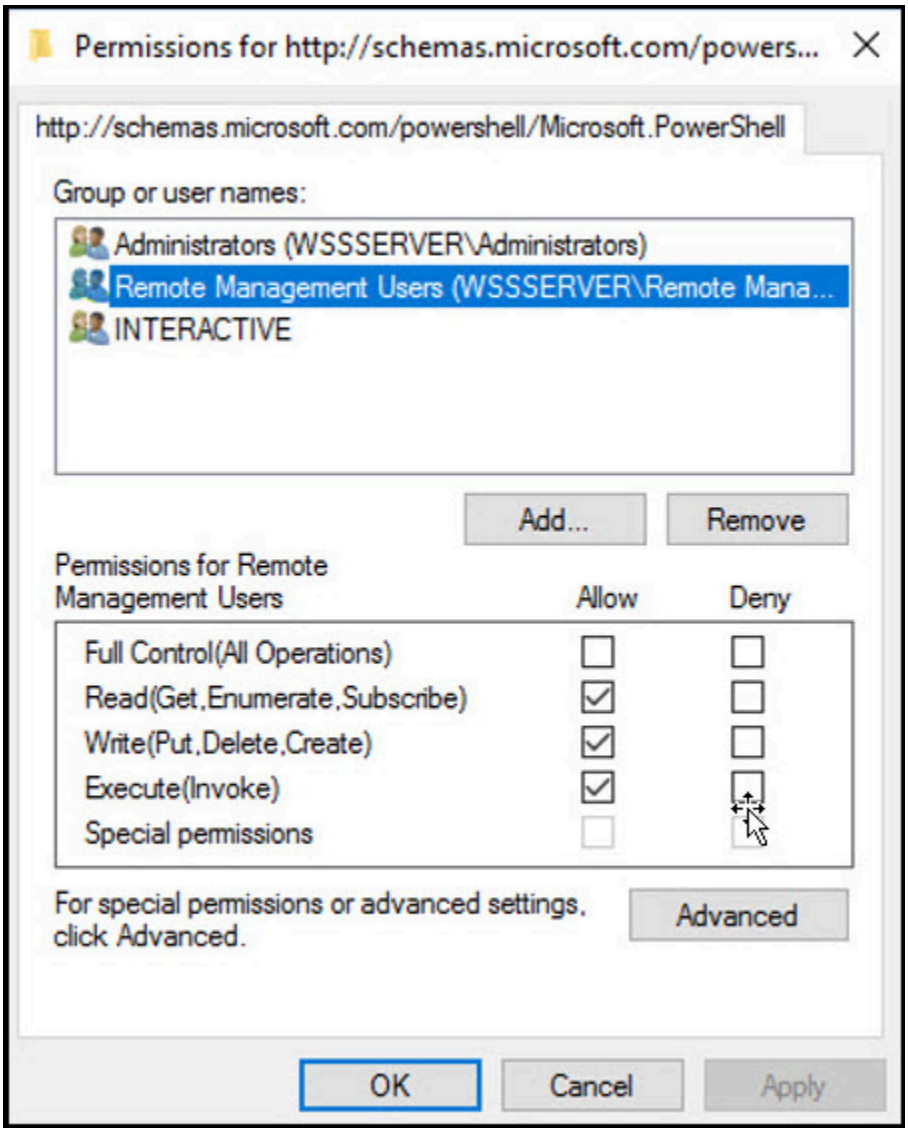
   The service account, for example: <waep_kerberos>, must be part of the Remote Management Users group.

3. To validate if the Remote Management Users group has permissions to execute the scripts, run the below command on the AD server and the policy server:

```
Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell
```

4. Add the service account to the Remote Management Users group in AD.
5. Assign Read,Write, and Execute permissions to the group.

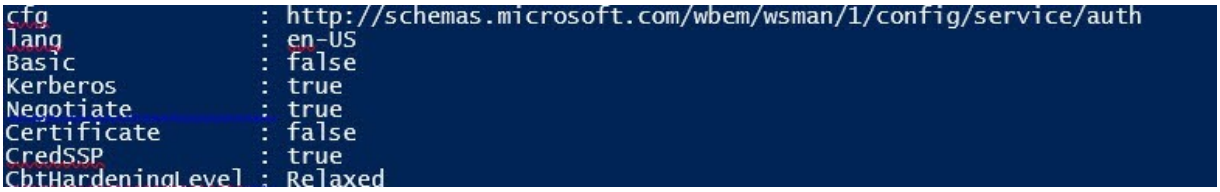
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Enable Credential Security Support Provider (CredSSP) authentication on the policy server (CEP/CES) and the AD servers by running the following command:

```
Enable-WSManCredSSP -Role Server
```

7. Once the server role is enabled, ensure the parameters, Kerberos, Negotiate, CredSSP, are set to *true* and CbtHardingLevel is set to *Relaxed* as shown:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Windows Auto-Enrollment Proxy

1. Log onto the AppViewX application using your credentials.
2. Go to (**Menu**) icon **> CERT+.**
   The CERT+ left navigation pane appears.
3. Expand the **Administration** menu and select **Auto Enrollment > WAEP.**
   The **Windows AEP** auto-enrollment page is displayed.
4. Click **+New Setting** to add a WAEP auto-enrollment request.
   The **Windows AEP : New Setting** page is displayed.
5. Enter the following fields:

Field Description for Windows AEP : New Setting page

Field	Description
Endpoint Details	
***Name**	Provide a unique name for the WAEP setting. **Note:** Only alphanumeric and the following special characters are allowed: period (.), hyphen (-), and underscore (_). The name cannot begin with a special character.
***Cloud Connector**	Select the hostname based on the domain.
***Data Center**	Field is auto-populated based on the Cloud Connector hostname.
Active Directory Configuration	
***Policy Server**	Provide the IP address or the hostname of the **Certificate Enrollment Policy Web Service (CEP)/ Certificate Enrollment Web Service (CES)** or policy server used to execute the remote Windows PowerShell scripts.
***LDAP Server**	Select or enter the hostname of the AD/LDAP server.
***Service Account with Base**	Provide the service account created for bind. For example: cn=test_service, ou=Kerberos_accounts, dc=avxtest, dc=com
***Service Account Password**	Provide the service account password.

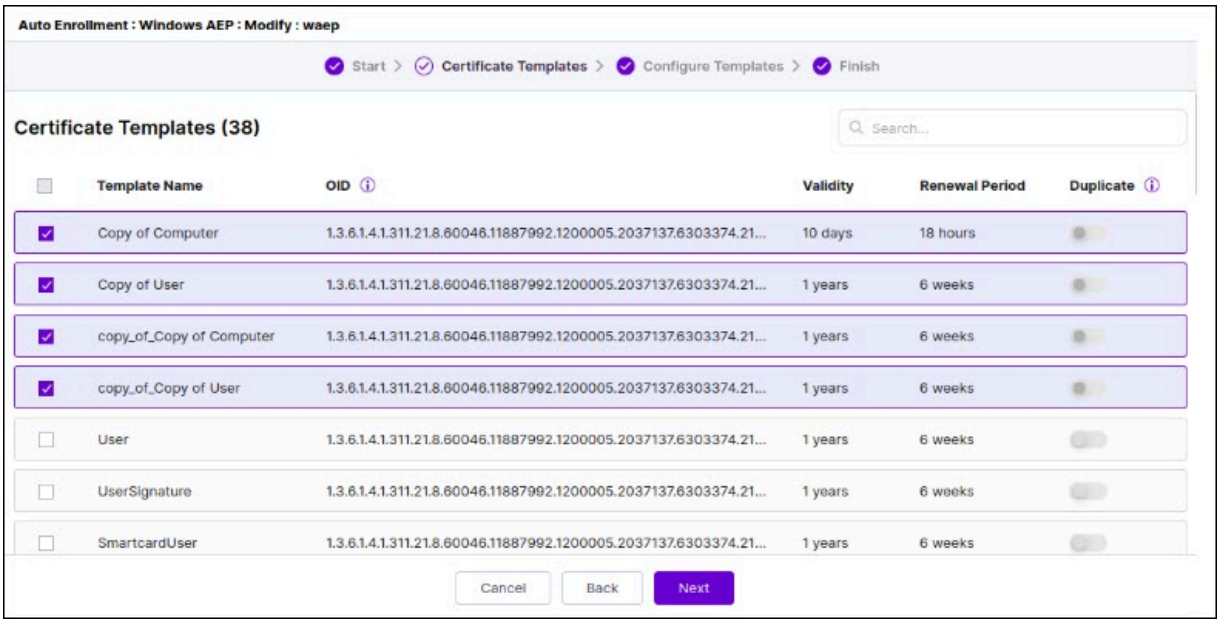
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Active Directory Sync	This field is optional for manual import of templates.Enable this toggle button to fetch all the global catalog servers in your forest. **Note:** Auto fetch and AD sync are present only for SaaS setup.
Global Catalog Configuration	
***Global Catalog Server IP**	If Active Directory sync is enabled, then this field lists all the global catalog servers in your forest as a dropdown list.
***Port**	Port 3268 is the MS default port for global catalog.
***LDAP Base DN**	If AD sync is enabled, the LDAP base DN is auto-populated based on the IP address of the global catalog server selected from the dropdown list.
Validate Account	Click the button to validate connection of the global catalog server with your service account credentials. If the validation is successful, you see *Success* displayed next to the button. If it fails, then check the service account credentials, or permissions to the global catalog server, or verify the global catalog server IP and try again.
Import Templates	
***Type**	By default, **Manual** is selected. It is recommended that you select the **Auto** option to automatically fetch your templates from your AD. If you have selected **Manual,** then drag and drop your template that you created or browse to the location it is saved. Auto-fetch is only supported in SaaS environment.
Fetch Templates	The templates are fetched and populated in the **Certificate Templates** screen.
Note: Fields marked with red asterisk (*) symbol are mandatory.	

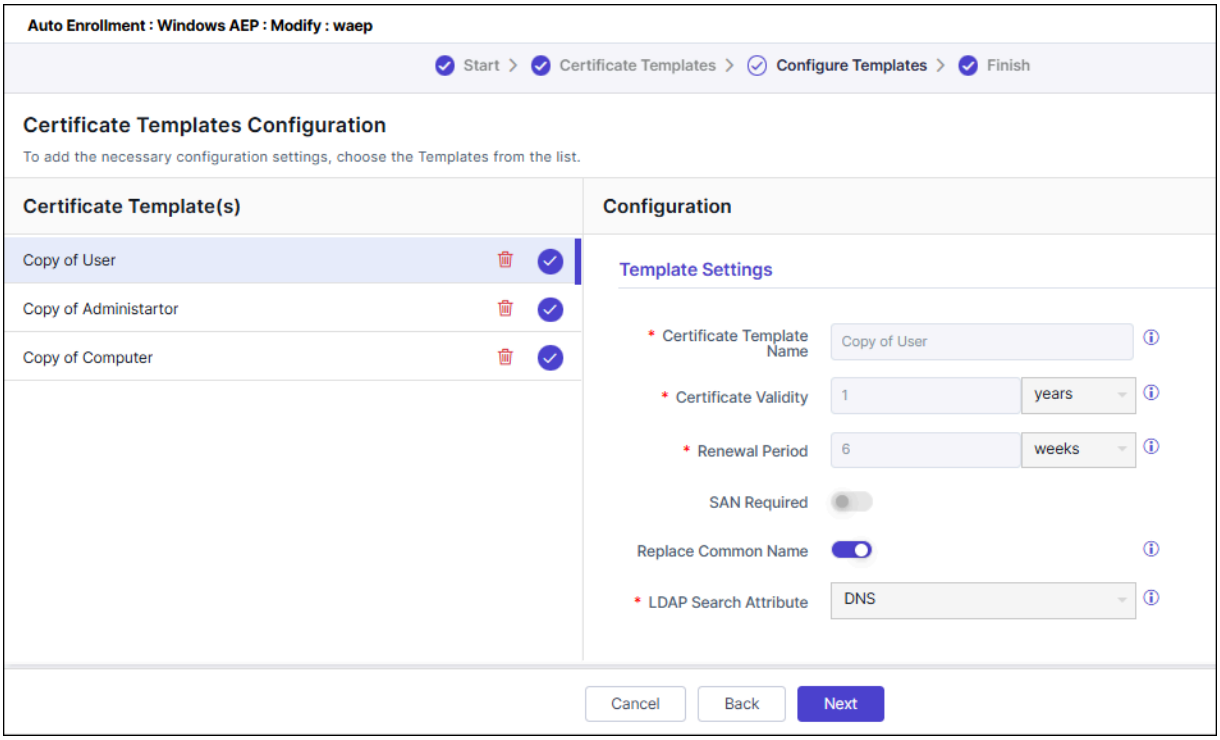
6. Click **Next.** A message that templates are imported successfully appears.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Certificate Templates** page appears along with all the fetched templates along with the details populated in the table as shown.



7. Select the templates you want to configure and click **Next.**
   The **Certificate Templates Configuration** page appears.
8. Click the template you want to configure and fill out the details in the **Configuration** page that appears on the RHS of the page.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Enter the following fields:

Field Description for Certificate Template Configuration page

Field	Description
Template Settings	
***Certificate Template Name**	Value is populated based on the auto-fetched or uploaded data.
***Certificate Validity**	Enter the expiry time limit for certificates.
***Renewal Period**	Enter the renewal time limit for the template.
SAN Required	This is disabled by default.
Replace Common Name	This is disabled by default. If enabled, the issued certificate's Common Name will be replaced with the value retrieved from the specified LDAP field name.
***LDAP Search Attribute**	This field appears only on enabling the **Replace Common Name** toggle. You can search the LDAP attribute by DNS, which is populated by default. This value will replace the Common Name in the issued certificate.
Subject Alternative Names	This field appears only when you select the **SAN Required** checkbox. Select from the following values: • DNS • Email • User Principal Name • Service Principal Name **Note:** You can either choose DNS/Email or both, or customized SAN such as User Principal Name/Service Principal Name or both. For example, if you select DNS/Email or both, you cannot select User Principal Name/Service Principal Name and vice versa.
***Certificate Profile**	This field will not appear for PKIaaS Native CA. Select the profile configured to set the Key Usage and EKU.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This profile must match the Key Usage values and EKU as seen in the actual on-prem Microsoft template in case of manual fetch.
CA Configuration	
***Certificate Group**	Select the certificate group for managing the certificates.
***CA Name**	Select a CA for WAEP to communicate for certificate enrollment.
***CA Account**	The field values are listed only when the account is added to CA settings.
***CA Certificate**	Select issuer certificate. It is recommended to select intermediate CA certificates to sign all the client certificates.
***Issuer Name**	Select the issuer name for the certificate.
***Issuer Location**	This field will not appear for PKIaaS Native CA. Select the issuer location for the certificate.
***Template**	This field appears only for PKIaaS Native CA. Select from the dropdown list.

On completion, you get a message that the template is saved successfully and a blue tick mark appears across the configured template.

Note:

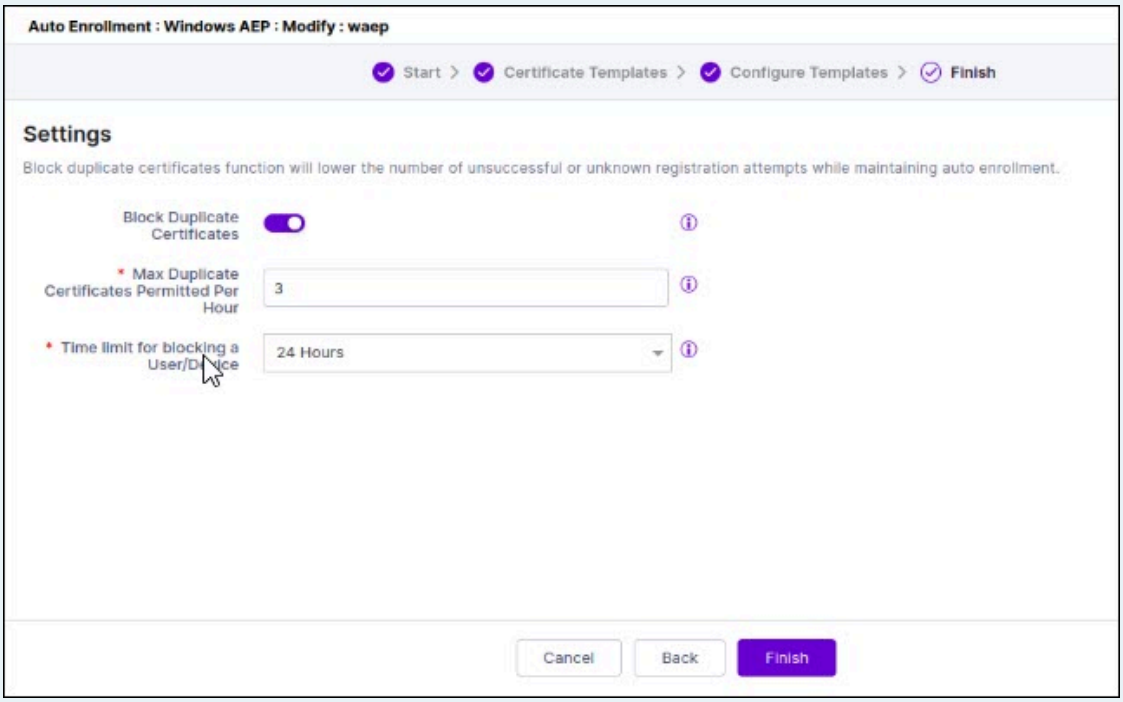
- You can select or clear the templates by going back to the previous page.
- You cannot click **Next** until all the selected templates are configured.
- Click the (**Delete**) to delete a selected template.

10. Click **Next.**

    The **Settings** page appears. By default, the **Block Duplicate Certificates** toggle button is disabled. If you enable it, you can customize the values for blocking the maximum number of duplicate certificates in an hour and the time limit to block a user/device issuing the certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: By default, the time limit for a user/device is 24h. If you change this value, ensure to update the **Occurrence Type** by navigating to **CERT+ > Administration > Job Scheduler** and selecting **Pkiaas AEP Purge log Job.** If you have set the time limit as 12h or 24h, then choose **Occurrence Type** as **Daily.** For values more than 24h, choose **Occurrence Type** as **Weekly.**

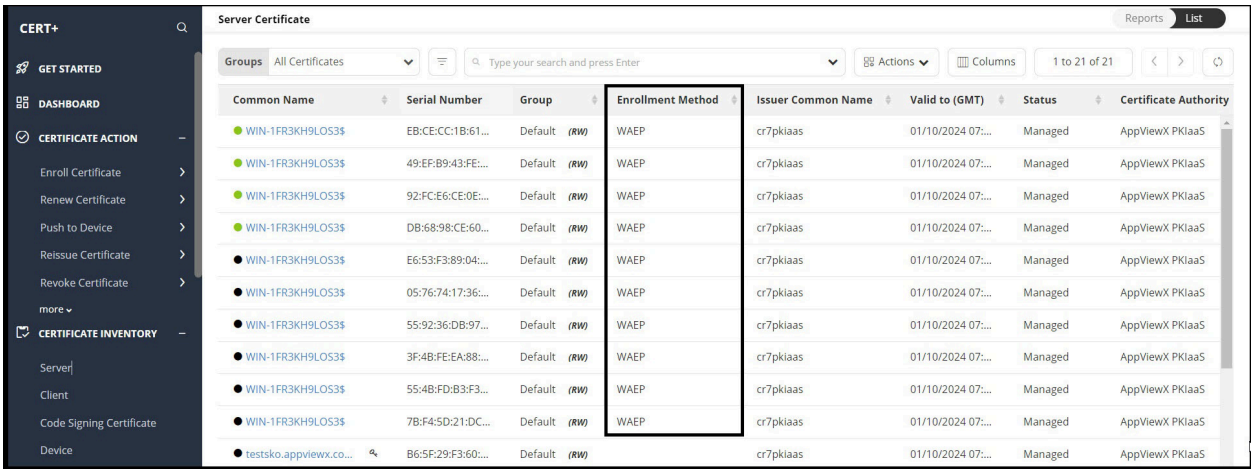


11. Click **Finish.**

    A message that the WAEP settings is saved successfully appears.

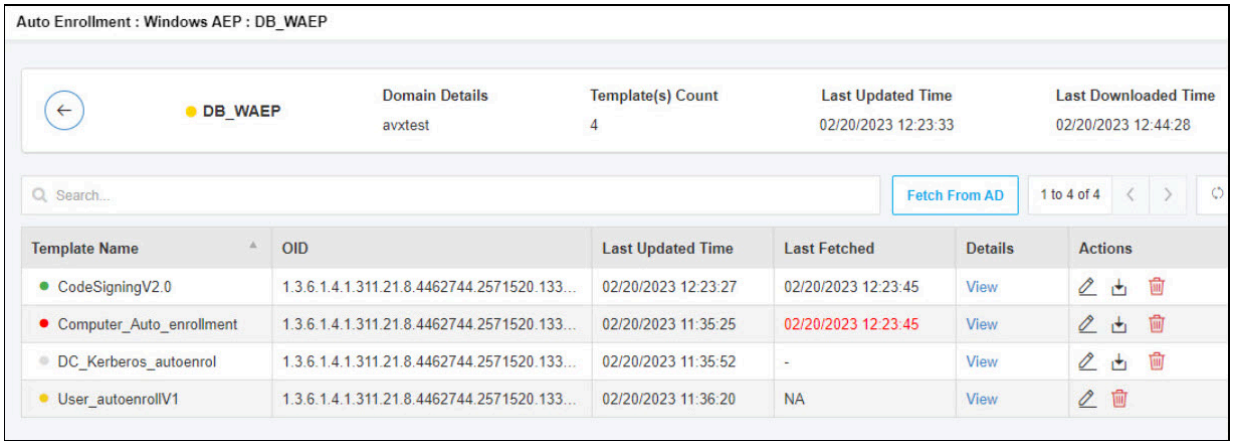
The AppViewX PKIaaS certificates that are auto-enrolled via WAEP appear on the **Cert+ > Certificate Inventory** page as shown. You can filter the AppViewX PKIaaS certificates using the WAEP enrollment method.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



What to do next:

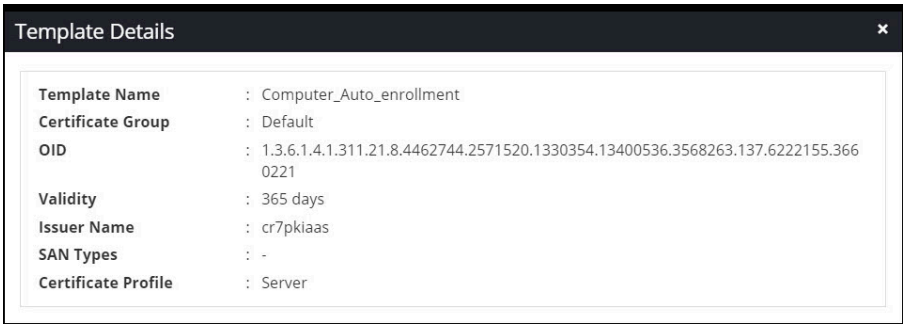
- [Applicable only if you have chosen automatic upload of template] Click **Download** to download the entire set of configured certificate template scripts and the runnable files to publish on your active directory.
- Click **Go to Inventory** to view the added WAEP setting on the dashboard.
- Click the **Endpoint Setting** hyperlink on the dashboard to view details of the configured certificate template.



- Once the templates are fully configured, click **Fetch from AD** to fetch the templates from the active directory. A message, *Template sync triggered successfully,* appears. Here are the color codes against the templates:
  - **Green:** indicates the templates were fetched successfully along with the last fetched time.
  - **Amber:** indicates the templates are partially configured. The last fetched time will be NA.
  - **Gray:** indicates the templates were not found in the AD or the templates not yet published. The last fetched time will be empty for these.
  - **Red:** indicates the templates were deleted along with the last fetched time.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Click **View** to get the certificate template details.



- Click the (**Edit**) icon to edit configuration of the certificate template.
- Click the (**Download**) icon to download a selected template, or click the (**Delete**) to delete a selected template.

- Viewing the added WAEP Setting on the Dashboard
- Updating AppViewX CES URL
- Verifying AppViewX CES URL
- Certificate Enrollment Validation using AppViewX PKI

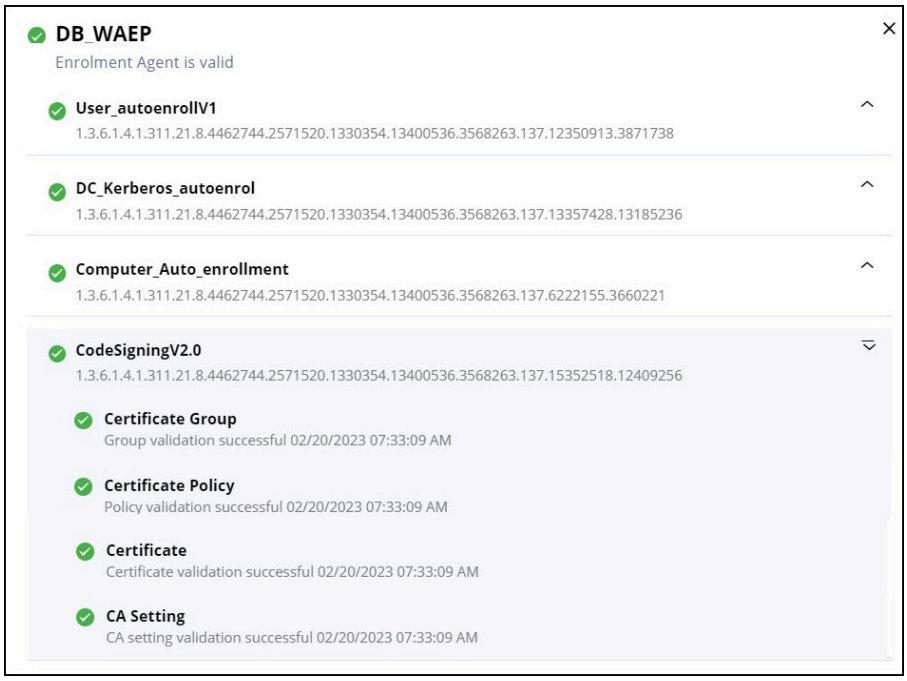
Viewing the added WAEP Setting on the Dashboard

To view the newly added WAEP setting on the dashboard:

1. Click **Go to Inventory** to view the added WAEP setting on the dashboard.
2. From this page, you can do any of the following actions:
   - Click **Check** to check if the certificate template configuration is successful. If the certificate template configuration is successful, the status changes to *Valid,* else it turns to *Invalid*. For incomplete template certificate configuration, the status shows as *Incomplete.* To complete the WAEP configuration, click the (**Edit**) icon.

     You can also expand to view the validation attributes and status of the connection separately for each of the certificate templates as shown:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- If the certificate is found in the enrolled Windows client machine, then the enrollment is successful and the **Success Requests** tab on the dashboard is incremented by 1. If it is unsuccessful, then the count in the **Failed Requests** tab is incremented by 1.
- If you have enabled the **Block Duplicate Certificates** on the **Settings** page, then based on the value set for the permissible duplicate certificates in an hour further auto-enrollment requests are blocked for the day with a log entry, *Duplicate Certificate request - Certificate entry with this Common Name, Certificate Template and SAN value has already been issued.* The user/device is automatically unblocked after the set time limit has elapsed.

  The administrator can manually enable the blocked user/device from the WAEP page by clicking **View** in the **Blocked Users** tab, selecting the checkbox against the user name to unblock, and clicking **Unblock.**

  Click the **Audit Log** to get details on the unblocked user/device. The details include the device/user name, domain, date and time on when it was blocked and unblocked, and who unblocked it. You can also download the audit log in the CSV format.

- Click the (**Edit**) icon to edit the WAEP configuration.
- Click the (**Delete**) to delete the WAEP configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Updating AppViewX CES URL

Once UI configurations are done and successful we can proceed to update the Windows Auto-Enrollment Server URL on ADCS.

1. Log onto the CEP machines using your service account.
2. Open a command prompt on the CEP windows machine.
3. To get the current URL, run:

```
certutil -config <FQDN\MSCACN> -enrollmentserverurl
```

4. Ensure to replace the server <FQDN> and <MSCACN> names with CEP machine's FQDN and MSCA common name.
5. Copy the URL displayed in the output of the previous command, which looks like https://<CEP-FQDN>/<CA-NAME>_CES_Kerberos/service.svc/CES.
6. To remove the existing enrollment server URL, run:

```
certutil -config <FQDN\MSCACN> -enrollmentserverurl https://<CEP-FQDN>/<CA-NAME>_CES_Kerberos/service.svc/CES delete
```

7. To add the new enrollment server URL, run:

```
certutil -config <FQDN\MSCACN> -enrollmentserverurl https://<CC\Appviewx-Hostname>:<Port-Number>/avxapi/msproxy/simpleenroll Kerberos
```

8. Ensure to replace the server <CC\Appviewx-Hostname> and <Port-Number> before running the previous command.

Verifying AppViewX CES URL

To get the current URL, run the command in CEP:

```
certutil -config <FQDN\MSCACN> -enrollmentserverurl
```

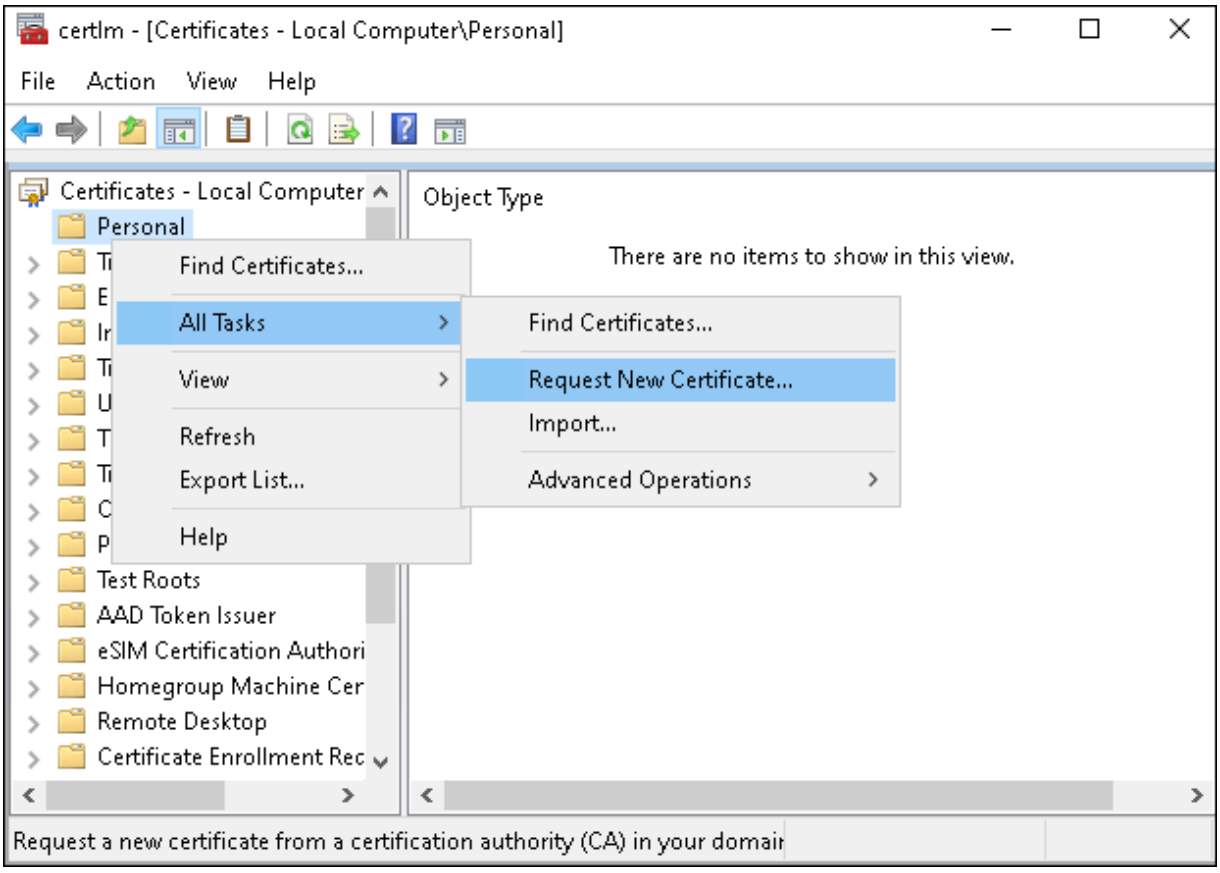
Note: The output of the previous command must be the AppviewX URL configured in the previous step.

Certificate Enrollment Validation using AppViewX PKI

1. **Login to the Client Machine**
   Open **MMC** and add **Computer** and **User Snap-ins**.
2. **Request a New Certificate**

   Navigate to the **Personal Store**, right-click, and select **Request New Certificate** as shown below:

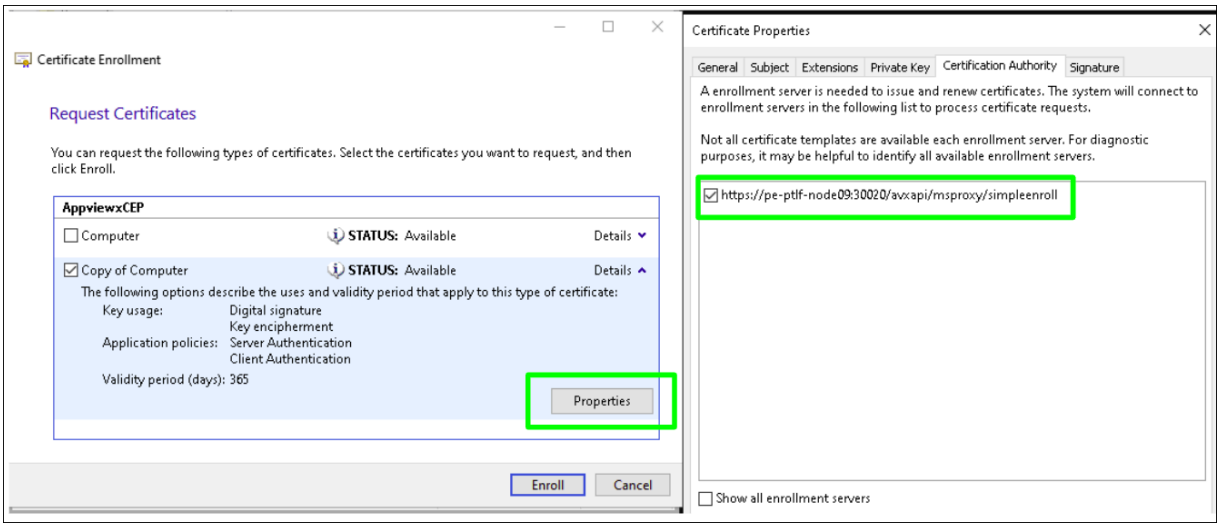
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Select the configured **CEP Server** and choose the template set up in the AppViewX GUI for enrollment.

3. **Verify CES URL Update**

   Open the template properties and check if the CC URL is listed under the **Certificate Authority** tab as shown below:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. **Complete Enrollment**
   - Click **Enroll** to proceed.

   The issued certificate will appear in both the **AppViewX Inventory** and the **Windows Certificate Store**.

AppViewX Enrollment Server

Introduction

The AppViewX Enrollment Server processes and automates certificate deployment and renewal for users and computers within an Active Directory domain. The process begins when the Windows autoenrollment client sends a certificate request to the AppViewX Enrollment Server. The server validates the request against the user's account in Active Directory, retrieving additional attributes as needed to meet template requirements defined by organizational policy. It then forwards the request to the Certificate Authority (CA), which processes it according to the certificate profile configured in the AppViewX UI. Once issued, the certificate is returned to the Enrollment Server and delivered to the requesting client. If enabled, the server can also publish the certificate to Active Directory for wider accessibility.

System Requirements and Service Account Configuration

1. **A valid Service Account with the below permissions**
   - Enterprise Admin
   - Domain Admin
   - Remote Management Users
   - Administrator
   - Domain User
2. **CC Service Setup**
   - Install ACME-HTTPS and SCEP-HTTP services on the CC.
   - Configure WAEP in the AppViewX GUI specific to CC.
3. **Domain Machine Requirements**
   - **SaaS Setup**
     - **Outbound Calls**
       - Port 30020 for unidirectional communication from domain machines to CC.
       - Port 30022 for CRL verification.
     - **Inbound Calls**
       - Port 5985 for auto-fetch requests from CC to the Enrollment Server machine.
   - **On-prem Setup**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Outbound Calls**
  - Port 31443 for unidirectional communication from domain machines to AppViewX Node from Enrollment Server Machine.
  - Port 30022 for CRL verification.

> **Note:** Auto fetch/lift and shift functionalities are only supported in the SaaS model.

4. **Domain and Connectivity**
   - AppViewX Enrollment Server must be in the same domain as the AD, with connectivity to the AD server.
   - Ensure a valid DNS record for the CC/AppViewX node exists in domain machines.
5. **Certificate and Trust Configuration**
   - Issue the certificate using AppViewX PKIaaS CA and enable trust on Windows domain machines.
   - Steps to add root and intermediate certificates to the Windows domain machines:
     a. Log onto the AD machine using your service account.
     b. Move the root and intermediate certificates that need to be trusted to the appropriate location.
     c. Open the command prompt with administrator privileges.
     d. To publish the **Issuing CA** certificate, run:

```
certutil -dspublish -f <PathToCertFile.cer> SubCA
```

     e. To publish the **Root CA** certificate, run:

```
certutil -dspublish -f <PathToCertFile.cer> RootCA
```

     f. Run the following command to force a policy update and push the certificates to the domain machines:

```
gpupdate /force
```

Configuring WAEP Templates

Templates can be fetched in two ways: manual and automatic. Fetching templates is essential for mapping each template to a specific CA configuration setting.

Manual Fetch Configuration

Prerequisites

- Generate CSV file (Applicable only for manual upload of templates)

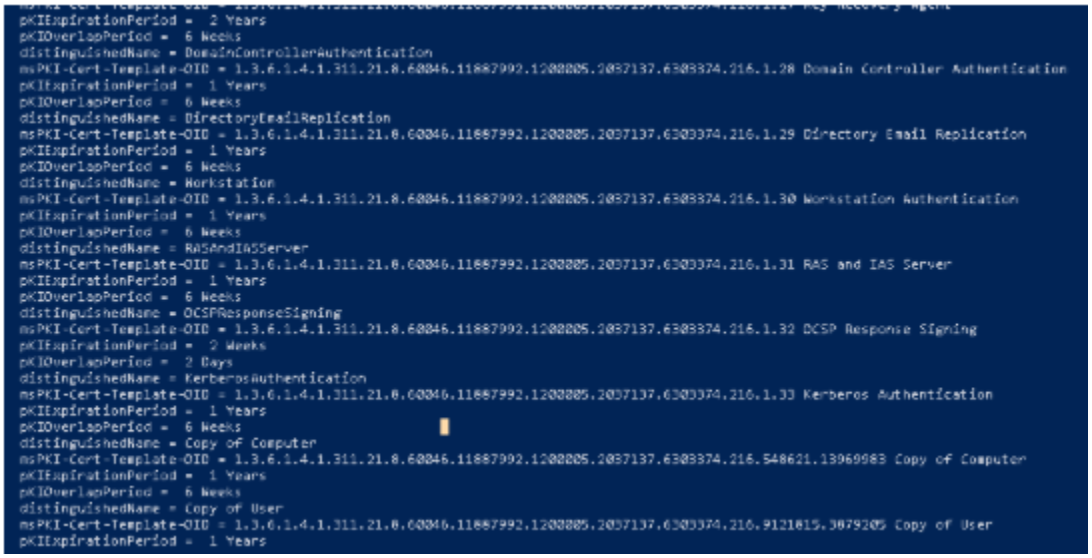
To generate CSV file:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Run Windows PowerShell.
2. To extract information of the certificate name, certificate template OID, validity period, and renewal period from the templates published on the ADCS server, run the command on the ADCS server:

```
Certutil -adtemplate -v | select-string distinguishedName,msPKI-Cert-Template-OID,pKIExpirationPeriod,pKIOverlapPeriod
```

3. Copy the certificate name, certificate template OID, validity period, and renewal period for Computer_Auto_enrollment template and User_autoenrollment template as shown.



> **Note:** The Copy of Computer template is used to enroll devices while the Copy of User template is used to enroll users.

4. Open a spreadsheet and create column headings:
   - **templateName:** In this column, add entries as Computer_Auto_enrollment template and User_autoenrollment.
   - **templateOID:** In this column, paste the OIDs copied in Step 3 against the respective template.
   - **validityPeriod:** In this column, enter the value as 365, which is the default value of the validity period.
   - **validityPeriodUnit:** In this column, enter the value as *days, weeks, months, or years*.
   - **renewalPeriod:** In this column, enter the value as 30, which is the default value of the renewal period.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The renewal period must be less than the validity period.

- **renewalPeriodUnit:** In this column, enter the value as *hours, days, weeks, months, or years*.

5. Once done, save the file in .xls, or .xlsx, or csv format.

Auto-Fetch Configuration

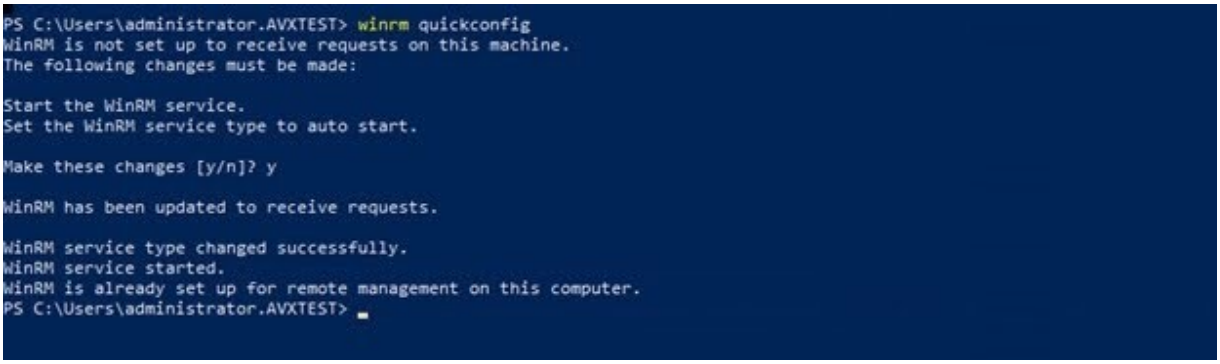
Templates can also be automatically fetched from the Windows machines using WAEP. To use auto-fetch:

Enable WinRM services in AD and AppViewX Enrollment machine

For the Lift & Shift feature to work, enable the WinRM service on the AppViewX Enrollment machine and the AD servers configured in WAEP for global fetch configuration and publication of templates.

To configure WinRM service (Applicable only for automatic upload of templates):

1. Run winrm quickconfig on the PowerShell window as an administrator.
2. Type *y* when prompted to start the WinRM service.



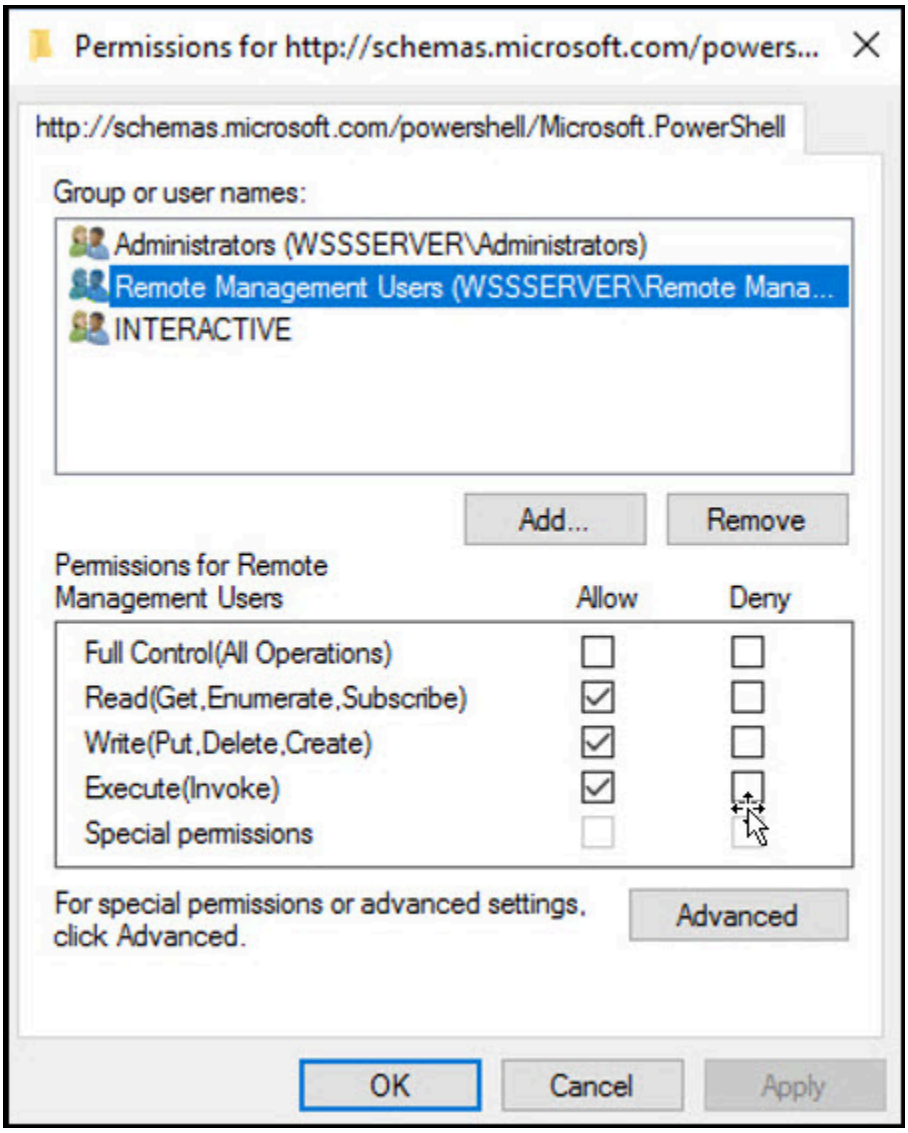
   The service account, for example: <waep_kerberos>, must be part of the Remote Management Users group.

3. To validate if the Remote Management Users group has permissions to execute the scripts, run the below command on the AD server and the AppViewX Enrollment Server:

```
Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell
```

4. Add the service account to the Remote Management Users group in AD.
5. Assign Read,Write, and Execute permissions to the group.

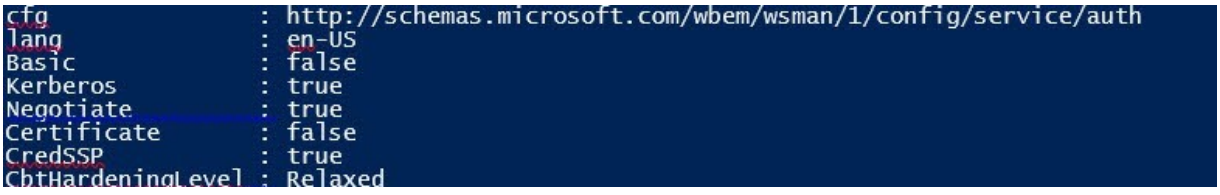
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Enable Credential Security Support Provider (CredSSP) authentication on the enrollment server and the AD servers by running the following command:

```
Enable-WSManCredSSP -Role Server
```

7. Once the server role is enabled, ensure the parameters, Kerberos, Negotiate, CredSSP, are set to *true* and CbtHardingLevel is set to *Relaxed* as shown:



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Windows Auto-Enrollment Proxy

1. Log onto the AppViewX application using your credentials.
2. Go to (**Menu**) icon **> CERT+.** The CERT+ left navigation pane appears.
3. Expand the **Administration** menu and select **Auto Enrollment > WAEP.** The **Windows AEP** auto-enrollment page is displayed.
4. Click **+New Setting** to add a WAEP auto-enrollment request. The **Windows AEP : New Setting** page is displayed.
5. Enter the following fields:

Field Description for Windows AEP : New Setting page

Field	Description
Endpoint Details	
***Name**	Provide a unique name for the WAEP setting. **Note:** Only alphanumeric and the following special characters are allowed: period (.), hyphen (-), and underscore (_). The name cannot begin with a special character.
***Cloud Connector /Host**	Choose the hostname of the Cloud Connector for SaaS deployments, or the hostname of the On-Premise Node where the MS-Proxy pod is enabled
***Data Center**	Select the data center.
Active Directory Configuration	
***Policy Server**	Provide the IP address or the hostname of the machine where AppViewX Enrollment Server is installed.
***LDAP Server**	Select or enter the hostname of the AD/LDAP server.
***Service Account with Base**	Provide the service account created for bind. For example: cn=test_service, ou=Kerberos_accounts, dc=avxtest, dc=com
***Service Account Password**	Provide the service account password.
Active Directory Sync	This field is optional for manual import of templates.Enable this toggle button to fetch all the global catalog servers in your forest.

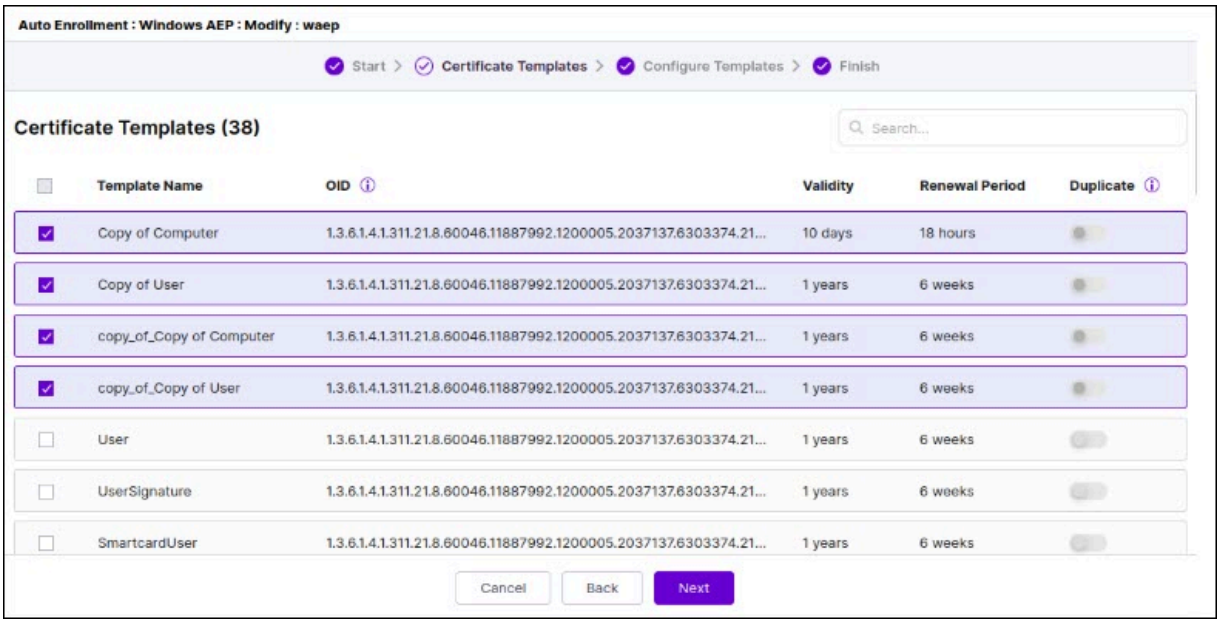
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This feature is available only for SaaS deployments.
Global Catalog Configuration	
***Global Catalog Server IP**	If Active Directory sync is enabled and it is applicable only for Saas deployments, then this field lists all the global catalog servers in your forest as a dropdown list. In case of non-SaaS based deployments, populate it with IP address of the AD machine. To enable the auto features for on-premise environments, install the cloud connector as an additional component.
***Port**	Port 3268 is the MS default port for global catalog.
***LDAP Base DN**	If AD sync is enabled, the LDAP base DN is auto-populated based on the IP address of the global catalog server selected from the dropdown list.
Validate Account	Click the button to validate connection of the global catalog server with your service account credentials. If the validation is successful, you see *Success* displayed next to the button. If it fails, then check the service account credentials, or permissions to the global catalog server, or verify the global catalog server IP and try again.
Import Templates	
***Type**	By default, **Manual** is selected. It is recommended that you select the **Auto** option to automatically fetch your templates from your AD. If you have selected **Manual,** then drag and drop your template that you created or browse to the location it is saved. For more details, see Configuring WAEP Templates.
Fetch Templates	The templates are fetched and populated in the **Certificate Templates** screen.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Note: Fields marked with red asterisk (*) symbol are mandatory.	

6. Click **Next.** A message that templates are imported successfully appears. The **Certificate Templates** page appears along with all the fetched templates along with the details populated in the table as shown.

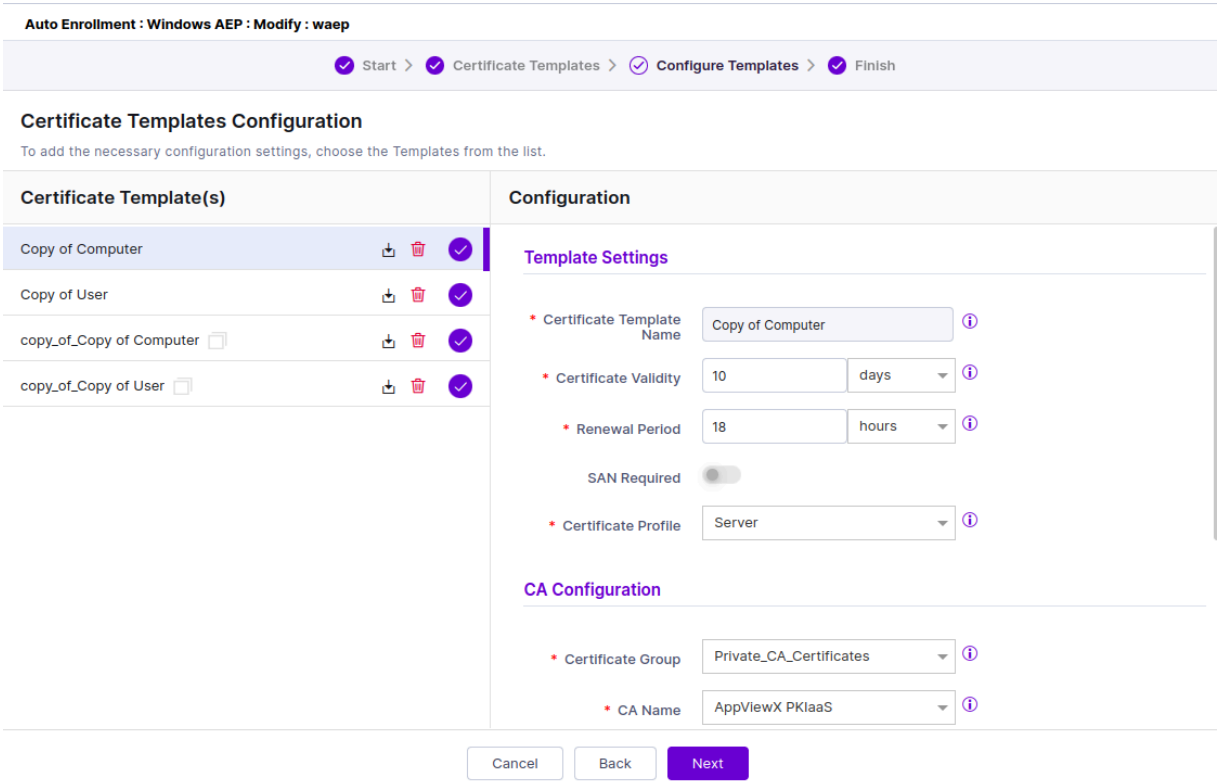


7. Select the templates you want to configure and click **Next.** The **Certificate Templates Configuration** page appears.

Note: [Applicable only if you have chosen automatic upload of templates] If you want to make a copy of an existing template, then select the checkbox against that template and slide the toggle button under the Duplicate column. The duplicated template name appears with the prefix: *copy_of_* along with the template name on the next page. For example, if you made a duplicate of the *DB_Test_Template* template, then the duplicate template appears with the name, *copy_of_DB_Test_Template*, which you can edit on the next page.

8. Click the template you want to configure and fill out the details in the **Configuration** page that appears on the RHS of the page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



9. Enter the following fields:

Field Description for Certificate Template Configuration page

Field	Description
Template Settings	
***Certificate Template Name**	Enter the name of the certificate template if you created a copy of it.
***Certificate Validity**	Enter the expiry time limit for certificates.
***Renewal Period**	Enter the renewal time limit for the template.
SAN Required	This is disabled by default.
Subject Alternative Names	This field appears only when you select the **SAN Required** checkbox. Select from the following values: • DNS • Email • User Principal Name • Service Principal Name

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: You can either choose DNS/Email or both, or customized SAN such as User Principal Name/Service Principal Name or both. For example, if you select DNS/Email or both, you cannot select User Principal Name/Service Principal Name and vice versa.
***Certificate Profile**	Select the profile configured to set the Key Usage and EKU. **Note:** This profile must match the Key Usage values and EKU as seen in the actual on-prem Microsoft template in case of manual fetch.
CA Configuration	
***Certificate Group**	Select the certificate group for managing the certificates.
***CA Name**	Select a CA for WAEP to communicate for certificate enrollment.
***CA Account**	The field values are listed only when the account is added to CA settings.
***CA Certificate**	Select issuer certificate. It is recommended to select intermediate CA certificates to sign all the client certificates.
***Issuer Name**	Select the issuer name for the certificate.
***Issuer Location**	Select the issuer location for the certificate.
***CA Connector Name**	By default, this is a CA Connector. If you created a CA connector manually, then provide that name here.

On completion, you get a message that the template is saved successfully and a blue tick mark appears across the configured template.

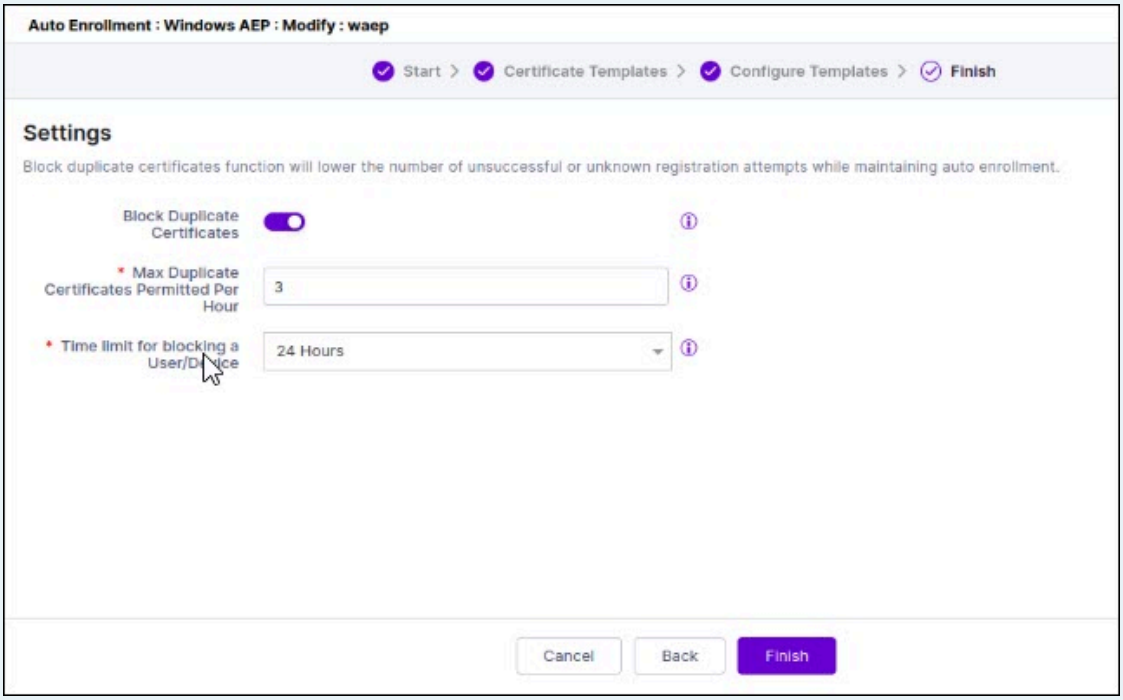
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- You can select or clear the templates by going back to the previous page.
- You cannot click **Next** until all the selected templates are configured.
- Click the (**Download**) icon to download a selected template (appears only if you have chosen automatic upload of templates) or click the (**Delete**) to delete a selected template.

10. Click **Next.** The **Settings** page appears. By default, the **Block Duplicate Certificates** toggle button is disabled. If you enable it, you can customize the values for blocking the maximum number of duplicate certificates in an hour and the time limit to block a user/device issuing the certificates.

Note: By default, the time limit for a user/device is 24h. If you change this value, ensure to update the **Occurrence Type** by navigating to **CERT+ > Administration > Job Scheduler** and selecting **Pkiaas AEP Purge log Job.** If you have set the time limit as 12h or 24h, then choose **Occurrence Type** as **Daily.** For values more than 24h, choose **Occurrence Type** as **Weekly.**



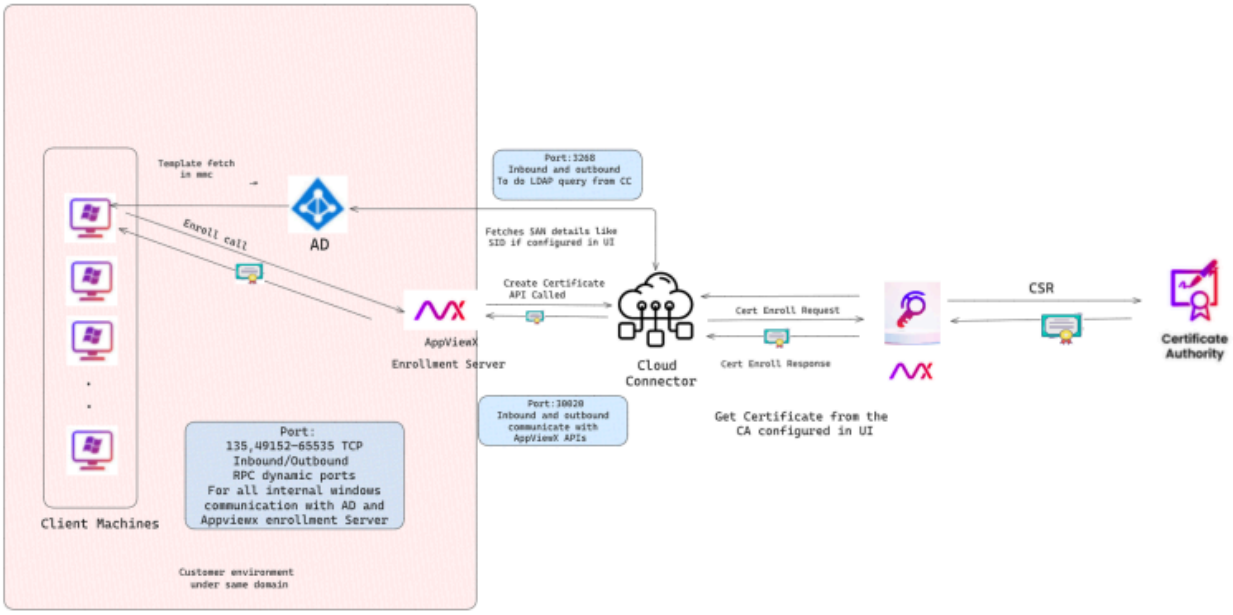
11. Click **Finish.** A message that the WAEP settings is saved successfully appears.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Auto-Enrollment Proxy

Introduction

The AppViewX Enrollment Server is a service that runs on a Windows machine, automating the deployment and renewal of certificates for users and computers within an Active Directory domain.



Prerequisites

- **Recommended Operating Systems:** The following operating systems are supported for client and server installations of the AppViewx Enrollment Server.

Role	Operating System
Client Machines(Machines requesting for Certificates)	Windows 10
	Windows 11
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
Server(Machines were AppViewX enrollment Server can be installed)	Windows Server 2016
	Windows Server 2019

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Role	Operating System
	Windows Server 2022

- **Software**

  2.1 .NET Framework

  - **Version:** .NET Framework 4.7.1
  - **Download Link:** Microsoft Download Center
- **Hardware**

  Recommended System Requirements

  - **Memory:** 16 GB RAM
  - **Hard Disk:** 100 GB available space
  - **Processor:** Quad-core or higher
- **Preparing the Windows Environment**

  Domain and Active Directory Requirements

  - A domain admin account is required for installing the AppViewx Enrollment Server.
  - A service account with admin privilege is required to perform LDAP queries from Appviewx and to fetch global configuration.
  - The AppViewX Enrollment Server machine must be installed in a Microsoft Windows domain with at least one Domain Controller.
  - Do NOT install the AppViewX Enrollment Server on the same machine running Microsoft Certificate Authority Services.
  - **Adding the Certificate Template Snap-In**

    Install the Certificate Template Snap-In for mmc to edit certificate template permissions. Follow the steps to add the certificate template snap-on as a domain administrator:

    1. Go to **Start > Administrative Tools > Server Manager.**
    2. Right-click **Server Manager** and select **Add Features.**
    3. Open **Remote Server Administration Tools > Role Administration Tools > Active Directory Certificate Services Tools** and select **Certification Authority Tools.**
    4. Click **Next.**
    5. Click **Install.**
  - **Allow Publishing to Active Directory**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The computer that runs the AppViewX Enrollment Server must be a member of the Active Directory group Cert Publishers for all domains, including the root domain. This grants the server the necessary permissions to publish newly issued certificates to Active Directory.

To add the server's computer account to the Cert Publishers group on machines with the Active Directory Domain Services role enabled:

1. Log on as the AppViewX Enrollment Server Administrator or as another user who is a member of the Enterprise Administrators group.
2. Go to **Administrative Tools > Active Directory Users and Computers.**
3. In the tree view on the left, expand your domain and click **Users.**
4. In the right panel, double-click the **Cert Publishers** group and go to the **Members** tab.
5. Click **Add** and add the computer account for the server running the AppViewX Enrollment Server. (You may need to include Computers in the Object Types filter to search for the computer name.)
6. Repeat these steps for the Cert Publishers group in every domain across your forest, including the root domain.

   For the new group membership to take effect, run this command on the machine where the AppViewX Enrollment Server is installed:

   ```
   gpupdate /force
   ```

- **Network and Firewall Requirements**

Required Ports

The machines using Enrollment server to request certificates must have the following ports open for communication with the AppViewX Enrollment Server:

Port	Protocol	Direction	Purpose
135	TCP	Inbound/Outbound	RPC endpoint mapper
49152–65535	TCP	Inbound/Outbound	RPC dynamic ports

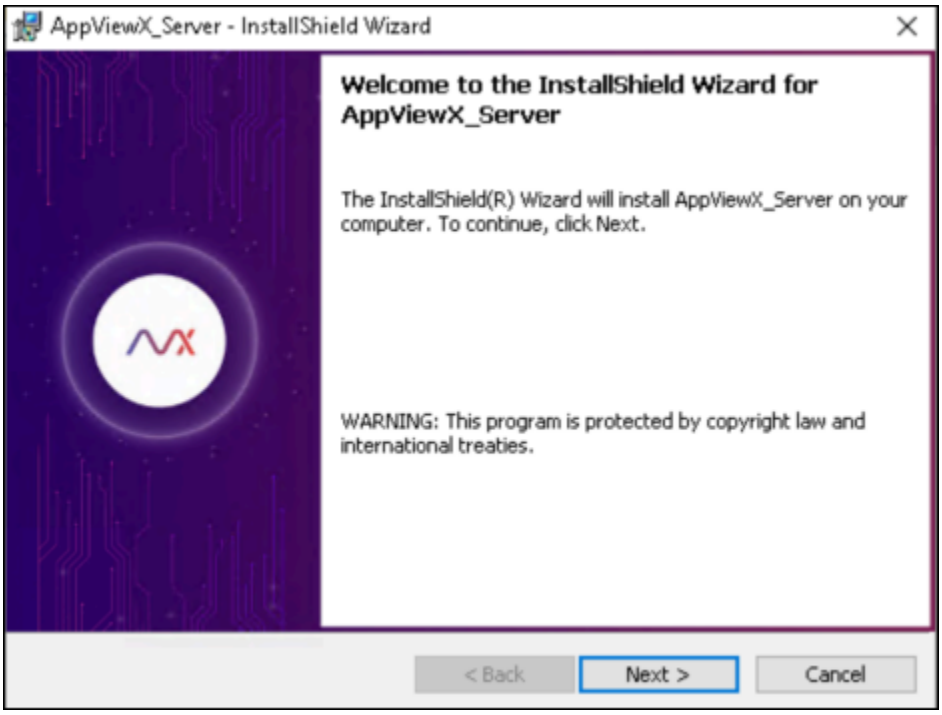
Note: The Enrollment server machines require both inbound and outbound access through port 30020 to communicate with the AppViewX APIs and request certificates from the CA.

Port 3268: Between the CC and the AD/LDAP server (used for LDAP queries if the template needs any ldap values to be embedded in SAN field or SID values).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

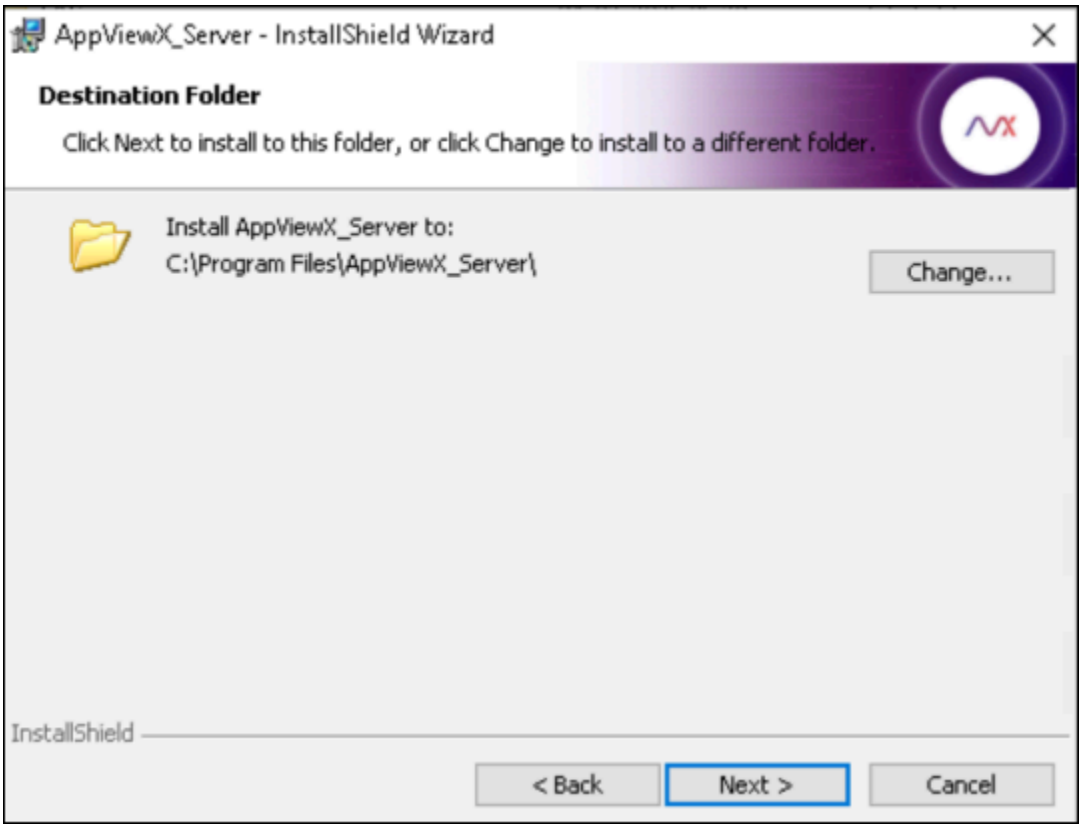
Installing AppViewX Enrollment Server

1. **Download:** Download the Appviewx_Enrollment_Server.zip file.
2. **Extract:** Extract the contents of the downloaded Appviewx_Enrollment_Server.zip file. Locate and extract the Appviewx_Enrollment_Server.exe file.
3. **Run as Administrator:** Right-click the Appviewx_Enrollment_Server.exe file and select **Run as administrator** to start the installation process and register it as a server.
4. **Welcome/Next:** In the installation wizard, select **Next** to proceed.



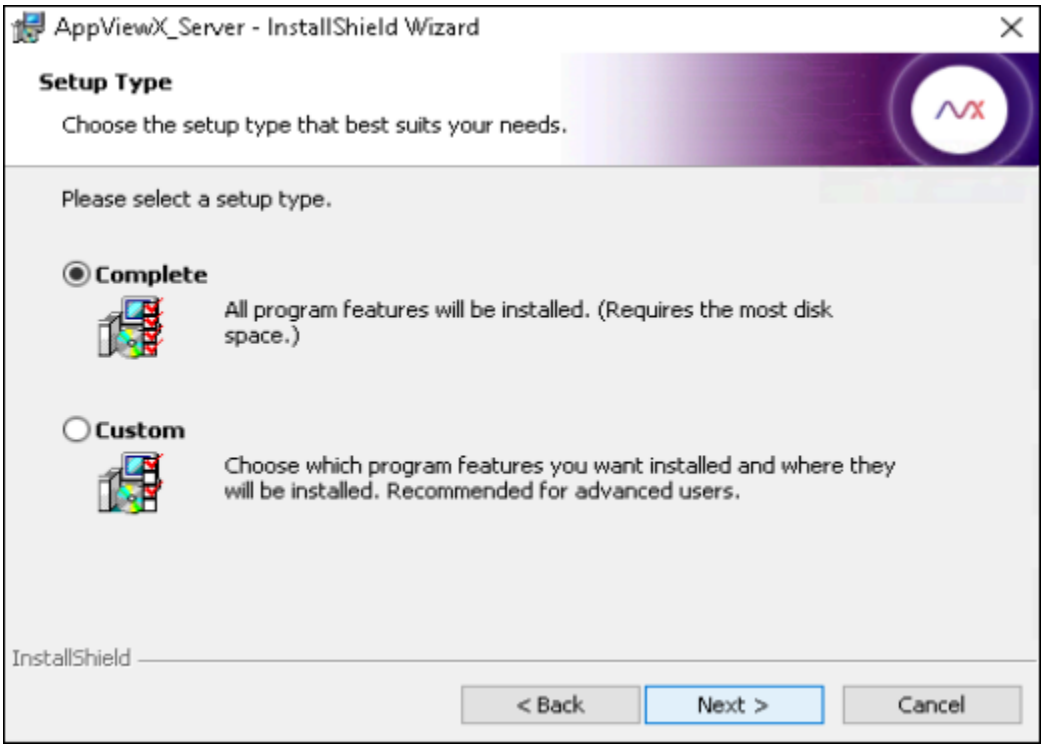
5. **Accept Agreement:** Accept the license agreement and select **Next**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. **Select Installation Location:** Choose the installation location for the service. The default location is recommended to be **Program Files (x86).** Select **Next** after choosing the location.
7. **Complete Installation:** Select the **Complete** installation option to proceed with the standard installation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

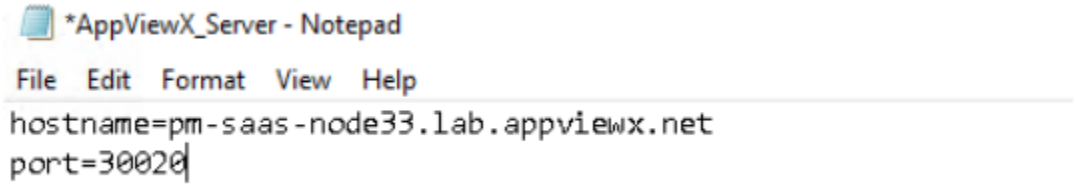


8. **Finish:** Complete the installation process by following any remaining prompts and selecting **Finish.**
9. **Modify the config files:** The configuration files are located in the **Installation Directory**, typically C:\Program Files\AppViewX_Enrollment_Server.

Update the main configuration file

Path: AppViewX_Enrollment_Server.ini

- Modify the **hostname** field with the (hostname/ip) of AppViewX Cloud Connector if CC is deployed or the on-premises deployment node or in case of multi-node please enter the details of the node in which the **ms-proxy pod** is installed.
- Set the **port** value to 30020 if using SaaS, or 31443 if using an on-premises deployment, or 443 if using a Load Balancer.



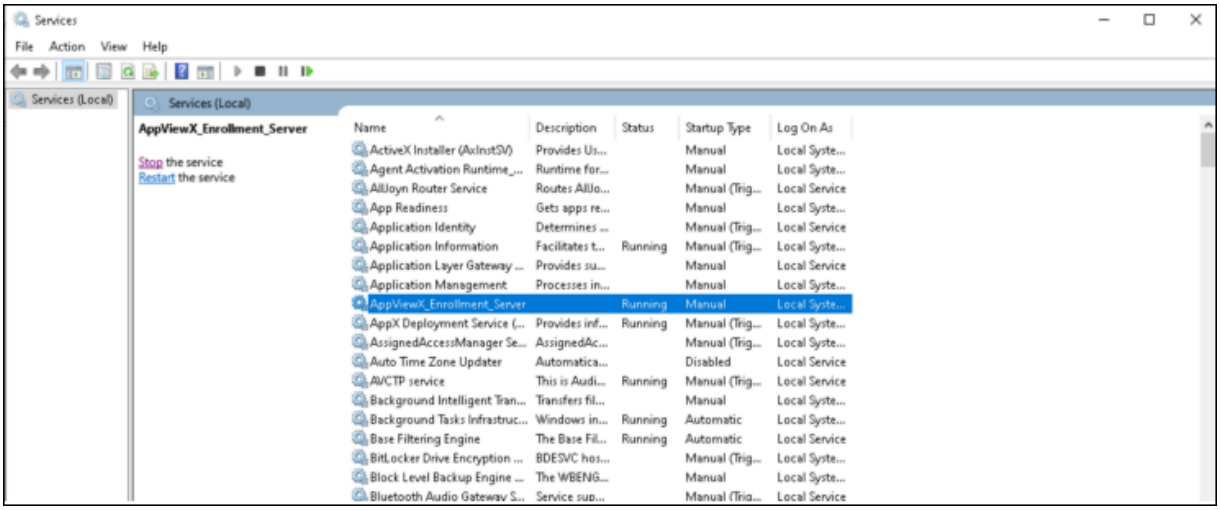
Update the client credentials file

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Path: Client_details.ini

- Update the **client-id** and **client-secret** fields with the CERT_AEP_SERVICE_ACCOUNT service account under platform tab in AppViewX GUI credentials.
- During the first-time setup client_id and client_secret_key are initially stored in plain text. On the first server startup, the client_id and client_secret_key are **automatically encrypted** and the file is updated securely.

10. **Start-Service:** Go to **Services** and start the **AppViewX_Enrollment_Server.**

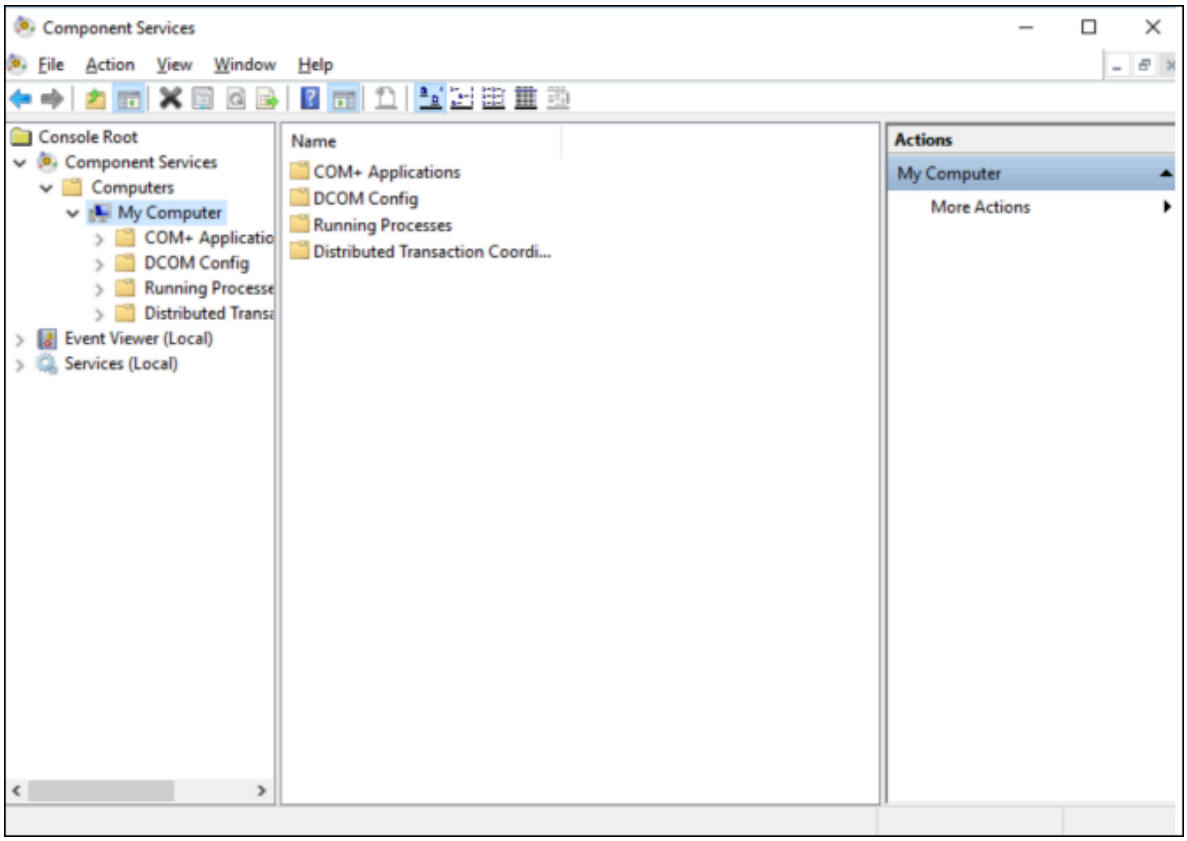


Configuring Permissions for AppViewX

1. **Enable DCOM on the Machine where the AppViewX Enrollment Server**
   a. Open **Component Services** from **Administrative Tools.**
   b. On the left pane, expand **Component Services > Computers > My Computer.**
   c. Right-click **My Computer,** select **Properties.**
   d. Go to the **Default Properties** tab.
   e. Ensure **Enable Distributed COM on this computer** is checked.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

f. Click **Apply** and then **OK.**



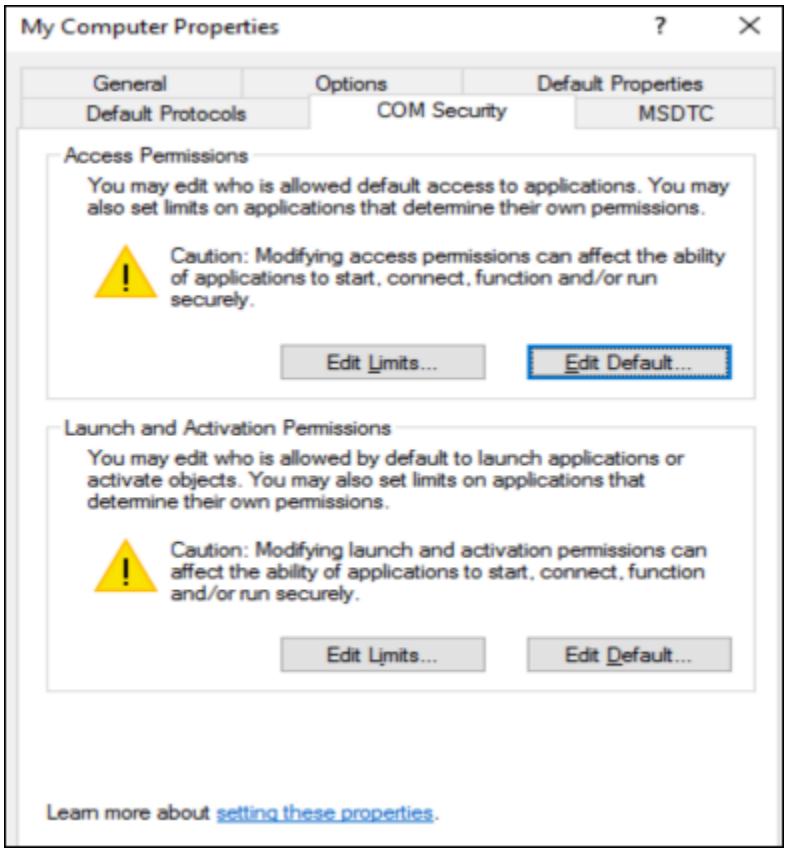
2. **Configure DCOM Access and Launch Permissions**

Set Global DCOM Access Permissions

a. Open **Component Services** again.

b. Right-click **My Computer** and go to the **COM Security** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



c. Under **Access Permissions,** grant **Local Access** and **Remote Access** to:
   - Domain Computers
   - Domain Controllers
   - Domain Users

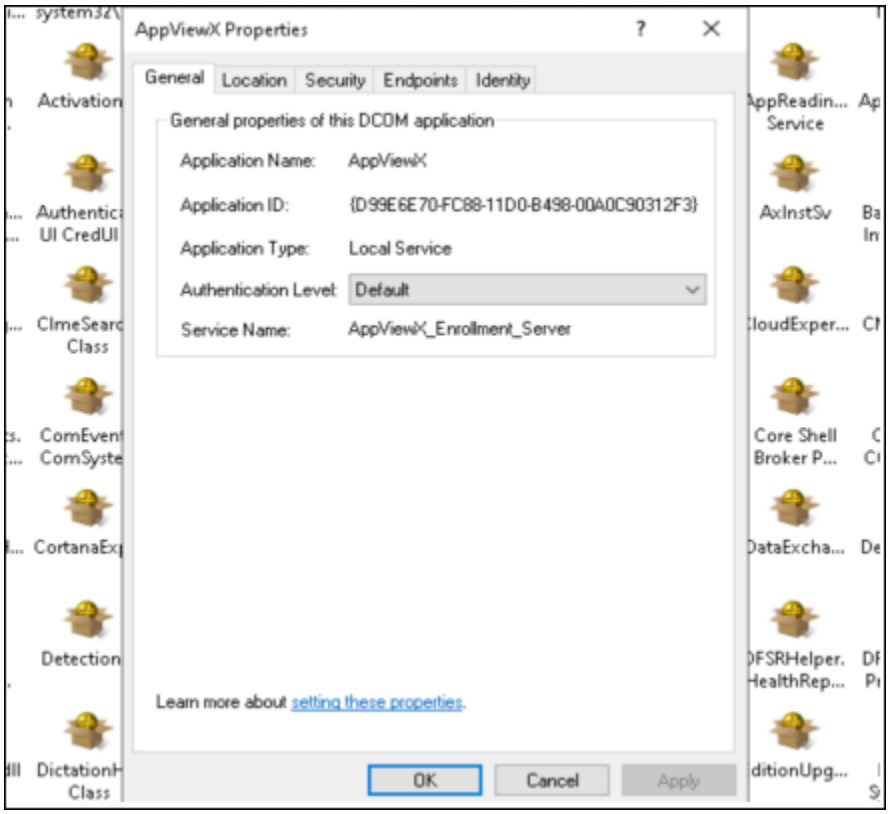
d. Under **Launch and Activation Permissions,** click **Edit Limits:**
   - Grant **Local Activation** and **Remote Activation.**
   - **Do not** select **Local Launch** or **Remote Launch.**
   - Apply the same permissions to:
     - Domain Computers
     - Domain Controllers
     - Domain Users

3. **Set Permissions for AppViewX Enrollment Server**

a. In **Component Services,** expand **DCOM Config.**

b. Find and right-click **AppViewX,** select **Properties.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



c. Go to the **Security** tab.

Launch and Activation Permissions:

- Choose **Customize** and click **Edit.**
- Grant **Local Access** and **Remote Access** to the same groups.
- Apply to:
  - Domain Computers
  - Domain Controllers
  - Domain Users
  - or Everyone, if no special security requirements exist

Access Permissions:

- Choose **Customize** and click **Edit**.
- Grant **Local Access** and **Remote Access** to the same groups.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Adding CA as Enrollment Service in AD

1. Run the following PowerShell command in the AD Machine with admin privileges and respective CA name and Domain name.

```
$CAName = "<CA_NAME>"
$Hostname = "<Hostname of FAS Machine>"
$Domain = "<Domain name>"

$domainComponents = $Domain.Split(".")
$DNComponents = $domainComponents | ForEach-Object {
"DC=$_" }
$DomainDN = ($DNComponents -join ",")

# Construct DN path for Enrollment Services
$DNPath = "CN=Enrollment Services,CN=Public Key
Services,CN=Services,CN=Configuration,$DomainDN"

# Construct FQDN for the CA machine dynamically
$CAAddress = "$Hostname.$Domain"


$certBase64 = @"
<BASE64 OF THE ROOT CA>
"@ -replace "`r`n", ""


$certBytes =
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
[System.Convert]::FromBase64String($certBase64)

# Get all certificate templates from Active Directory
$templates = Get-ADObject -Filter 'ObjectClass -eq
"pKICertificateTemplate"' `
    -SearchBase "CN=Certificate Templates,CN=Public Key
Services,CN=Services,CN=Configuration,$DomainDN" `
    -Properties Name
$templateNames = $templates | ForEach-Object { $_.Name }

# Create the AD object
New-ADObject -Name $CAName `
    -Type "pKIEnrollmentService" `
    -Path $DNPath `
    -OtherAttributes @{
        cACertificateDN     = "CN=$CAName,$DomainDN";
        dNSHostName         = $CAAddress;
        displayName         = $CAName;
        certificateTemplates= $templateNames;
        cACertificate       = $certBytes
    }
```

2. AD administrative access is also required for one time setup to run the PowerShell script to register the AppViewX Enrollment Service as **enrollment service object** within Active Director.
3. The **AD registering script template** file is attached in the installation directory of the enrollment server which can be used for registering.
4. Copy the full script and edit the values as needed. You can either paste and run it as one command in PowerShell or save it as a .ps1 file and execute that file.
5. Install the root certificate in the **Trusted Root Authority Cert Store** and publish it in domain using:

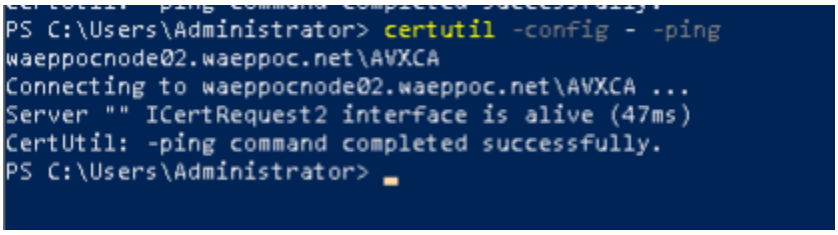
   ```
   certutil -dspublish -f <RootCA.crt> RootCA
   ```

6. **Test the AppViewX Enroll Server**

   Run the following PowerShell command select the **CA-Name** setup in the previous command:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
certutil -config - -ping
```



Adding Certificate Template to CA via ADSI Edit

1. **Open ADSI Edit**

   Press **Win + R,** type adsiedit.msc, and press **Enter.**

2. **Connect to the Configuration Naming Context**
   a. In ADSI Edit, right-click on ADSI Edit in the left pane and select Connect to.
   b. In the Connection Point, choose:

      Distinguished Name (DN) and enter:

      CN=Configuration, DC=yourdomain, DC=com (Replace yourdomain.com with your actual domain name)

3. **Navigate to the Enrollment Services Node**

   Expand the tree in the left pane:

   CN=Configuration, DC=yourdomain, DC=com

   → CN=Services

   → CN=Public Key Services 16

   → CN=Enrollment Services

4. **Select Your CA (Enrollment Service)**
   - Under **CN=Enrollment Services,** locate the object with the name of your CA (e.g., CN=YourCAName).
   - Right-click it and select Right-click it and select Properties.
5. **Edit the *certificateTemplates* Attribute**
   - On the **Properties** window, find the **certificateTemplates** attribute.
   - Click **Edit,** then click **Add** to add the name of the certificate template you want to support (e.g., User, Computer, CustomTemplateName).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. **Apply and Close**

   Click **OK** to close all dialogs and apply changes.

Log Location

The logs generated by the AppViewX Enrollment Server are stored in the C:\ProgramData\Appviewx_Enrollment_Server folder.

High Availability (HA) Setup

High availability can be achieved by installing the Enrollment Server on multiple machines. Certificate templates can be configured to requests through all deployed AppViewX Enrollment Servers, ensuring failover and load distribution.

Citrix FAS Integration

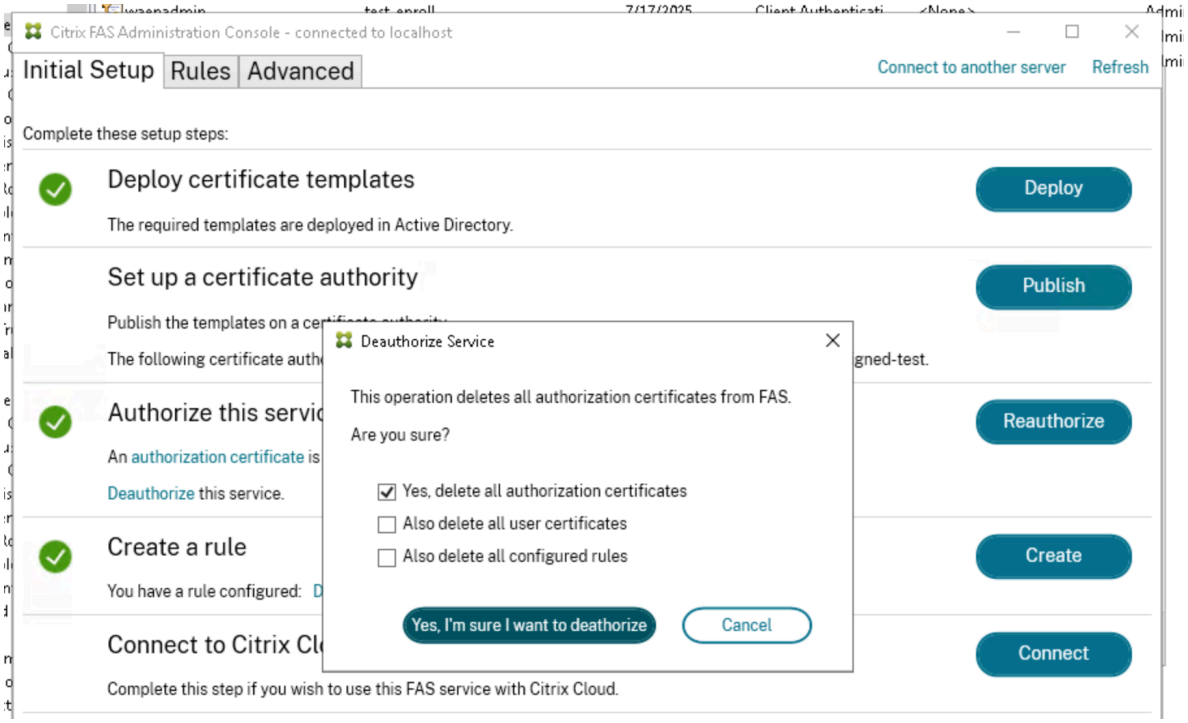
Configure Default FAS Rule

Ensure that the default FAS rule is updated to point to the Certificate Authority (CA) configured via the AppViewX Enrollment Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. **Obtain Authorization Certificate**
   a. **Remove Existing Authorization Certificate (If Already Configured)**: If an authorization certificate already exists:

      Open the Citrix FAS Console.



   b. Delete the existing authorization certificate.
2. **Generate Authorization Certificate Request**
   a. On the Citrix FAS server, run the following PowerShell command with administrator privileges:

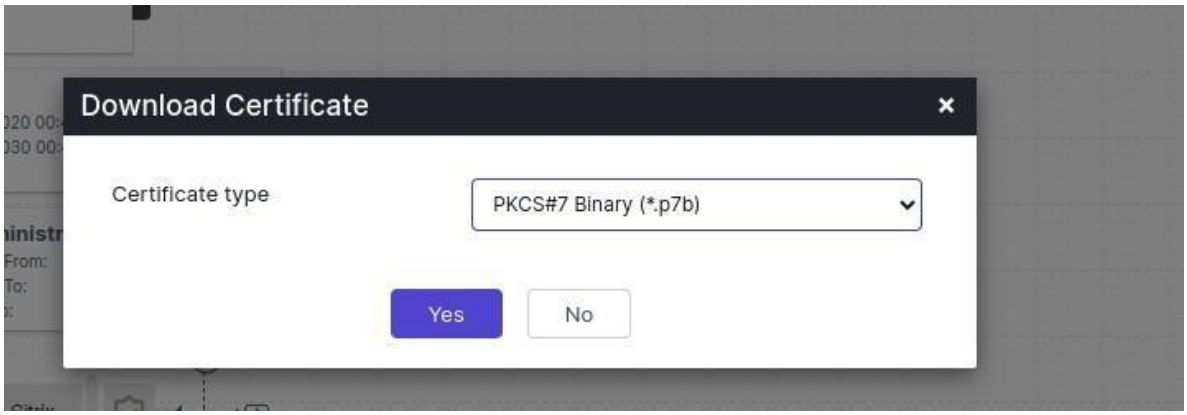
```
New-FasAuthorizationCertificateRequest -DistinguishedName "CN=<Administrator.account_name>.<Domain>.NET, O=<Domain>.NET"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

b. Replace <AdministratorAccountName> and <Domain> with appropriate values.

```
PS C:\Users\administrator.CTXFAS\Downloads\PSTools> New-FasAuthorizationCertificateRequest -DistinguishedName "CN=Admin
istrator.CTXFAS.NET, O=CTXFAS.NET"


Id                : c3a2171a-c099-41ca-8a29-c1772b6570d3
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE-----
                     MIICfTCCAWUCAQIwODETMBEGA1UEChMKQ1RYRkFTLk5FVDEhMB8GA1UEAxMYQWRtaW5pc3RyYXRv
                     ci5DVFhGQVMuTkVUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr1fMbSmn31t8zXre
                     r+Xy2RkAymGfUAAJmvHtZF5ScXhlZU8qBAYz1QEqFkscVvg1tdKhRnxh3Voz9taxDDWbNPZTGNeI
                     qARK5JPSGcnVzftimm+RdBoaFEsj8bOoe/KngFtmJb9Ztuoy68RTgP8GqtHMgQddhM3O4ePzNaS0
                     +VeOGRgONfezOCFFIV39xHdTH+PXtaqUA8e9lqTUtooy52+MPqdca0gispw/XPDmMt8Kj72azOTe
                     1KThCs7O3LP/uzXkoAW0BXafuu805OYcgM0MpZ2rcSyjaNSCbtEgrv4wXiWdN60NOfKjcAOQi+ph
                     iy3Sxt5MlDAyfp3w895i4QIDAQABoAAwDQYJKoZIhvcNAQENBQADggEBAESvD9oqp375qGCweQpp
                     b3BIyG+gZFG2doQxmQRI7OvMivmGs1CukVPGMBJ3/bL5zXf5fTi9O7hkmxWOU4+FFtMTNfmE188S
                     Bz4hpPSmmpIkNvL56Ie14E9+EzzyxYYyQd1+wMaXsdw1oBCMErhp8D4RL4n0ACIPZG7FbEzp9m6p
                     ZuuLHeYgIujTrWTdb11dBwni4Bzp5td4gIqkA/HyMZ6ePloIlP1Op1JcNYDiklRrYSbWl0L8MH0I
                     PmkYPFt5gvsqK1bCLB7aEMD9wspr5Deqx1XT0iSG8717rHhi2x+4Q02GNrU9oDBen4PPaqywoRyw
                     u5KGIddiZg+3j3ODeLA=
                     -----END CERTIFICATE-----
Status            : WaitingForApproval
```

3. **Submit CSR to AppViewX**
   a. Copy the generated Certificate Signing Request (CSR).
   b. Navigate to the Certificate page in the AppViewX Cert+ UI.
   c. Upload the CSR and download the issued certificate in PKCS#7 (.p7b) binary format.



4. **Import the Authorization Certificate**
   • Run the following command to import the certificate response:

```
Import-FasAuthorizationCertificateResponse -Id <IdFromPreviousCommand> -Pkcs7CertificateFile "<PathToCertificate.p7b>"
```

The Id is the value returned from the New-FasAuthorizationCertificateRequest command.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
Import-FasAuthorizationCertificateResponse    -Id    <id  from the previous
command>
-Pkcs7CertificateFile "<Path to your .p7b file>"
```

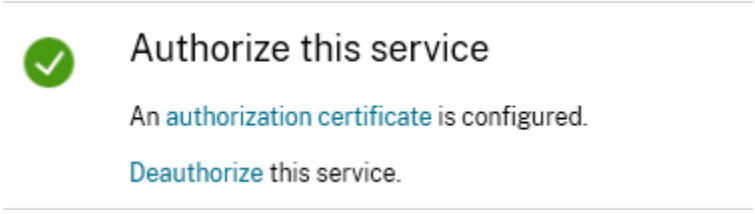
Note: The ID is acquired from the first powershell command

5. **Apply Changes in FAS Console**

   Open the FAS Console and click **Update Configuration** to apply the new authorization certificate.

   Result

   The authorization certificate is now successfully installed and applied to the Citrix FAS server.



6. **Test Smart Card Certificate Issuance**

   To validate the setup, run the following PowerShell command:

```
New-FasUserCertificate -UserPrincipalName "<user@domain.net>" -Rule Default -CertificateDefinition Default_Definition
```

Troubleshooting

General Errors

General errors that can be encountered

1. Global catalog validation fails in AppViewX GUI

Description	When an invalid ACME endpoint URL is provided in Posh-ACME, it will result in the following error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Validation fails in GUI.
Troubleshooting	• Check if CC is up and running. • Ensure that the service account's full name is the same as the login name as mentioned in the section.

2. CA Certificate not trusted in the windows domain machines	
Description	This error occurs when the issuer certificate of the bound certificate with CC is not trusted by the Windows domain machines.
Error	ERROR_WINHTTP_SECURE_INVALID_CA 12045
Troubleshooting	Ensure that both the issuing certificate authority (CA) certificate and the root CA certificate are added to the appropriate trust stores on each end machine. To implement trust at the domain level, see Point 6 within Section, System Requirements and Service Account Configuration .

3. Error when retrieving policy in windows domain machines	
Description	This error occurs when there is a connectivity issue between the CEP and end machines.
Error	**Error**An error occurred while obtaining certificate enrollment policy. **URL:** https://cepces.axxwaep.net/ADPolicyProvider_CEP_Kerberos/service.svc/CEP **Error:** The operation did not complete within the time allotted. **0x803d0006 (-2143485946)WS_E_OPERATION_TIMED_OUT**
Troubleshooting	• Check that the CEP server's certificate is valid. [IIS manager > Sites > Default site > Right click Edit bindings > check if the cert bound with 443 is valid]. If it's not, replace it with a valid one. Make sure the certificate's issuer is trusted by the domain machines. • Ensure that the CEP server hostname is resolved to the correct IP address from the end machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. An error occurred while enrolling for a certificate.

The certificate request could not be submitted to the certification authority.

Description	The error has occurred because either a firewall is interrupting the connection between the CC and the end machine, or a network device is filtering and preventing the certificate data from reaching its destination.
Error	**Error:** An error occurred while enrolling for a certificate. The certificate request could not be submitted to the certification authority. **URL:** https://testDomain:30020/avxapi/msproxy/simpleenroll **Error:** The operation did not complete within the time allotted. **0x803d0006 (-2143485946) WS_E_OPERATION_TIMED_OUT**
Troubleshooting	• Enable outbound traffic from domain machines to the Cloud Connector (CC) or AppViewX server on port 30020 for SaaS deployments and 31443 for on-premises deployments. • If a certificate is enrolled in the AppViewX GUI but not received by the Windows machine, verify that no network devices are blocking the certificate content.

Actions

You can perform any of the following actions on the EST, ACME, SCEP, MS Intune, or CMP agents:

- **Clone:** You can clone an existing agent with the same configuration settings under a new name, making it easy to duplicate and modify the setup without changing the original configuration.
- **Delete:** You can delete an agent by clicking the (Delete) icon and confirming deletion.

To clone an existing agent:

1. Click the **Clone** icon against the agent you want to clone.

   A confirmation window appears where you can enter the new name. By default, "_copy" is appended to the agent name being cloned.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click **Yes** to continue.

   A message appears that the agent has been cloned successfully.

3. To make changes to the existing configuration settings, click the cloned agent, make the changes, and click **Update**.

Note: When you clone an ACME agent, the **External Binding Account** field in the EAB Settings is set to **No** even if the setting was Yes in the agent being cloned.

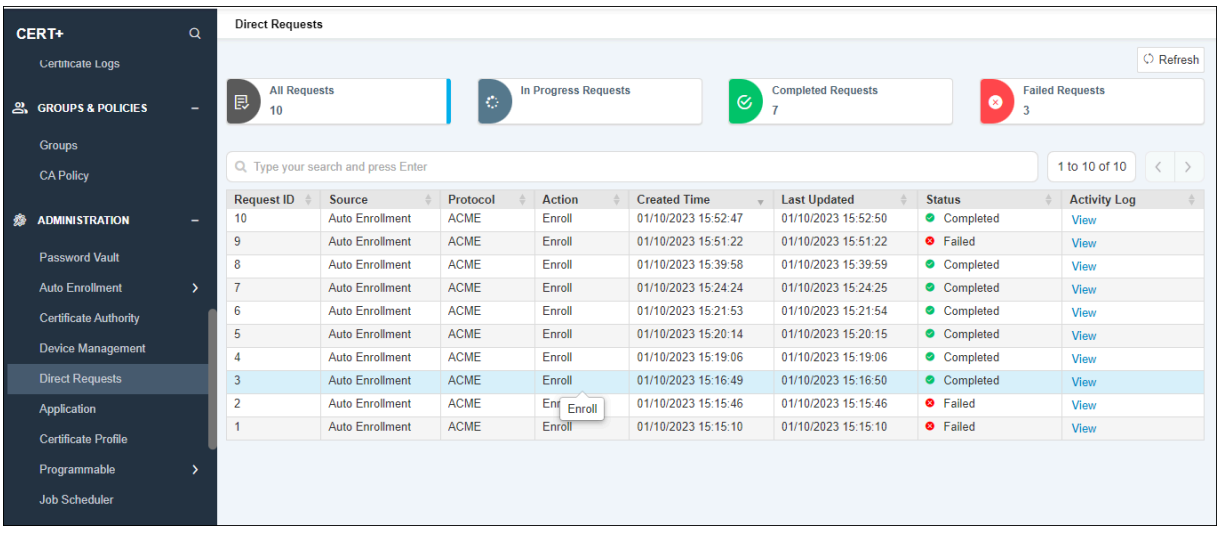
Direct Requests

The Direct Request page lists the auto-enrollment certificate requests for which the visual workflow will not be displayed for generating the certificates, resulting in a greatly improved performance. This page only displays the status and other details of certificate requests. No actions can be performed on this page.

Note: While creating an auto-enrollment request (for EST, ACME, SCEP, MS INTUNE), in the **Advanced Setting** section , select the radio button in **High Speed Transaction** field to “Yes” to display the requests in the Direct Requests page.

Accessing the Direct Request Page

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Direct Requests** .

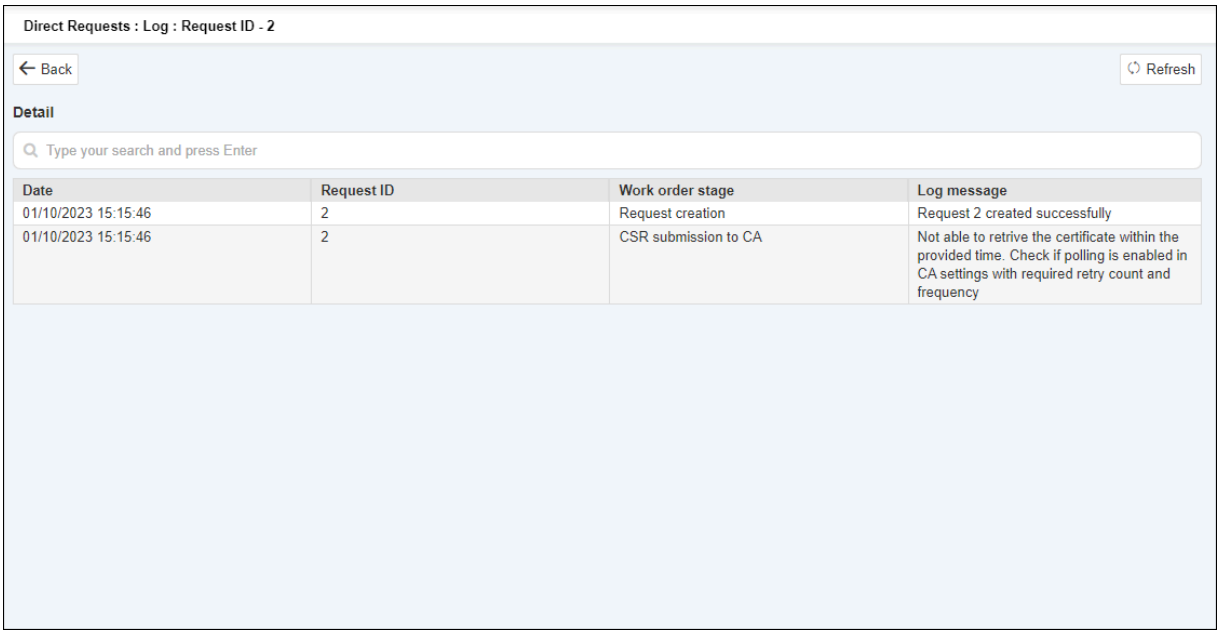


2. The Direct requests page displays the following:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Echelons** - All requests, In Progress Requests, Completed Requests, and Failed Requests. all echelons have the count of requests and are clickable. Clicking each echelon will display only those specific status requests.
- **Refresh** button
- **Search** field - users can enter values w.r.t. Request ID, Time Created, Request Status, CLM Action to search/filter for specific requests.
- Grid with the following columns -
  - *Request ID* - displays ID of the current request
  - *Source* - displays the source type, usually Auto Enrollment
  - *Protocol* - displays the type of protocol (EST, ACME, SCEP, MS INTUNE)
  - *Action* - displays the latest CLM action on the request
  - *Common Name*- displays the common name of the certificate
  - *Serial Number*- displays the serial number of the certificat
  - *Created Time* - displays the time the request was created
  - *Last Updated* - displays the time the request was last updated
  - *Status* - displays the status of the certificate request
  - *Activity Log* - displays the “View” link, when clicked displays the detailed logs at each status for the certificate request cycle.

An example of a failed request log is displayed below.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

MDM Device Integration for Certificate Lifecycle Management

• AppViewX Integration with JAMF

Integration of Mobile Device Management (MDM) with Auto-Enrollment Protocols

What is Mobile Device Management (MDM)?

Mobile Device Management (MDM) is a type of security software used by IT departments to monitor, manage, and secure employees' mobile devices such as smartphones and tablets. It involves the following steps:

- **Enrollment** - This step includes enrolling the mobile device into the MDM system. This can be done manually by the user or automatically through methods such as QR codes, email links, or by connecting to a company network.
- **Configuration** - Administrators create configuration profiles that define the settings and policies for the devices. These profiles can include Wi-Fi settings, VPN configurations, email settings, and more.
- **Deployment** - Once profiles and policies are created, they are pushed to the enrolled devices. This can happen over the air (OTA) through cellular or Wi-Fi connections.
- **Management** - Administrators can remotely manage the devices. This includes pushing updates, locking or wiping devices if they are lost or stolen, and troubleshooting issues.
- **Security** - MDM ensures that corporate data is protected through encryption, secure access controls, and the ability to remotely wipe data if a device is compromised.
- **Compliance** - Administrators can generate reports and audit trails to ensure compliance and for review purposes.

Benefits of using MDM with Auto-Enrollment Protocols

Mobile Device Management (MDM) systems often support auto-enrollment protocols like SCEP, EST, etc to streamline the process of enrolling devices into the management system. Auto-enrollment simplifies the initial setup for users and ensures that devices comply with organizational policies from the moment they are activated.

Benefits of using MDM with auto-enrollment protocols include:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Automation** - Automates the certificate issuance and renewal process, reducing administrative overhead and minimizing the risk of errors.
- **Scalability** - Easily scales to manage certificates for a large number of devices.
- **Seamless User Experience** - Provides a seamless experience for users, who don’t need to manually request or install certificates.

Use Cases

- **Wi-Fi Authentication** - Devices use certificates to authenticate to secure Wi-Fi networks, ensuring only authorized devices can connect.
- **VPN access** - Certificates authenticate devices when connecting to corporate VPNs, providing secure remote access.
- **Email encryption and signing** - Certificates enable secure email communications by supporting encryption and digital signing.
- **Application Authentication** - Certificates authenticate devices and users to enterprise applications, ensuring secure access to sensitive data.

AppViewX-supported MDMs

Some of the most popular MDMs that AppViewX integrates with are:

- **Microsoft Intune** - Part of the Microsoft 365 Suite, Intune provides comprehensive MDM and mobile application management (MAM) capabilities. Supports Windows, iOS, Android, and macOS devices.
- **Jamf Pro** - A leading MDM solution for Apple devices, widely used in enterprise and education settings. Supports macOS, iOS and iPadOS.
- **MobileIron** - A UEM platform that focuses on securing endpoints, apps, and cloud services. Support for iOS, Android, Windows, and macOS.

What's Next

AppViewX Integration with JAMF

What is JAMF

The advantages of using Jamf are as follows:

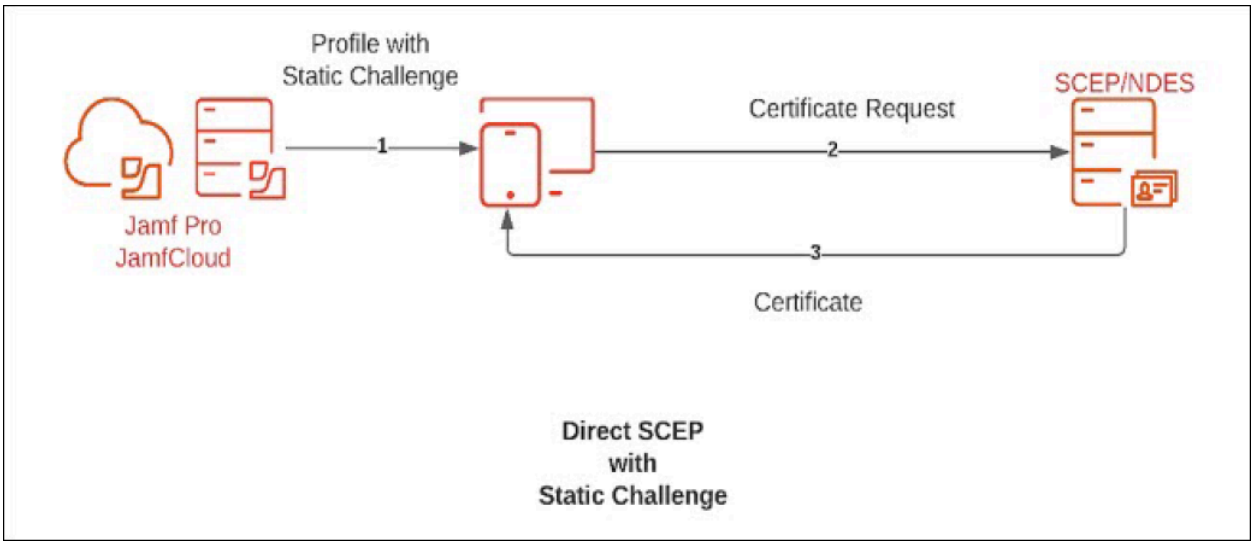
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **The Industry Standard for Apple Device Management** - The various products in the Jamf suite allow for seamless setup and deployment of devices, all offered in a single consolidated solution.
- **Cloud-Based Mobility** - Jamf Now is the ideal solution for small and medium enterprises as it empowers setting up, protecting, and managing devices right from one product.
- **Device Management Tool for The Pros** – An ultimate EMM (Enterprise Mobility Management) tool for your users. Jamf Pro features application and device management, deployment, security capabilities, inventory collection, and more.
- **Enhanced Identity Management** - Jamf Connect offers the flexibility to remotely and centrally manage passwords, groups, and users. It provides access to corporate cloud resources and applications that offer an advanced security and identity approach.
- **Mac-Exclusive Endpoint Protection** - Jamf Protect, developed natively on the iOS architecture offers deep visibility into any operations or threats at the endpoints. It has a dashboard, extensive reporting, and real-time alerts on the built-in security framework for macOS.

Deployment Models

SCEP obtains certificates from the CA and distributes them to managed mobile devices, providing a simplified way of handling large-scale certificate distribution. If you do not want computers or mobile devices to communicate directly with a SCEP server, you can configure settings that enable Jamf Pro to proxy the communication between a SCEP server and the computers and mobile devices in your environment. This allows Jamf Pro to communicate directly with a SCEP server to obtain certificates and install them on the device.

Jamf Pro can be configured using computers or mobile devices to communicate directly with a SCEP server.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

1. Disabling the checkbox in the **Global Management** > **PKI Certificates** screen.

   a. Login to JamfCloud (Sample URLs are mentioned below):
      i. **Cloud-hosted**— https://JAMF_PRO_URL.jamfcloud.com
      ii. **On-premise**— https://JAMF_PRO_URL.com:8443

   b. Click **Settings** > **All Settings** > **Global Management** > **PKI Certificates**.

   c. Ensure to disable the checkbox labeled **Enable Jamf Pro as SCEP Proxy for configuring profiles**.

   > **Note:** This is an important step to enable this deployment model.

2. Configure the **Challenge Password** in the **SCEP Configuration** and **AppViewX** endpoints.

   > **Note: Challenge Passphrase** is mandatory for MAC devices to connect to AppViewX SCEP Node.

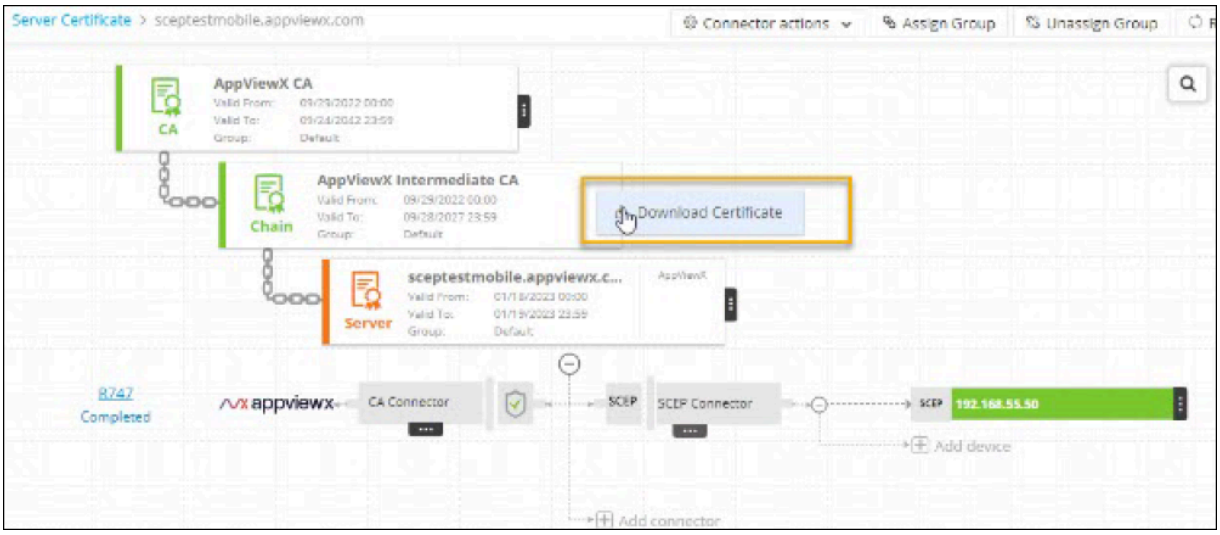
3. The MAC device should be able to connect to the SCEP server on port 30022.

Direct Communication with SCEP Server

Obtaining the Certificate Thumbprint/Fingerprint

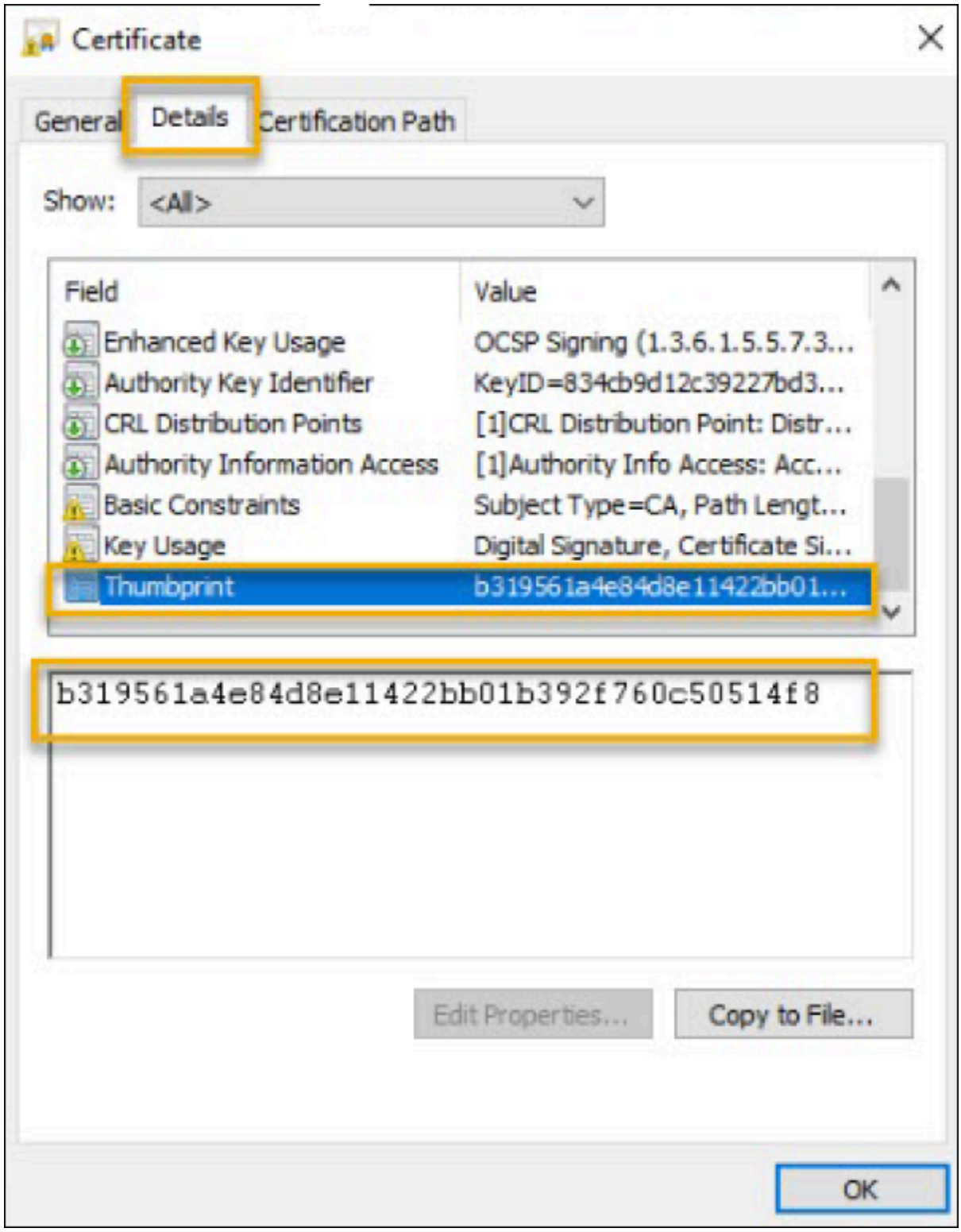
1. Log in to the AppViewX platform using valid credentials.
2. Hover on the menu icon and select CERT+.
3. Click **Certificate Inventory** on the left menu and select the certificate type (Server, Client, or Code Signing).
   The certificates with the common names are displayed on the right.
4. From the **Common Name** column, click on the desired certificate.
   All valid certificates are displayed.
5. Click the desired RA certificate to display the details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



6. Click the three dots on the issuer certificate to display the **Download Certificate** option.
7. Click **Download Certificate** and save the certificate in the desired format.
8. Open the downloaded certificate.

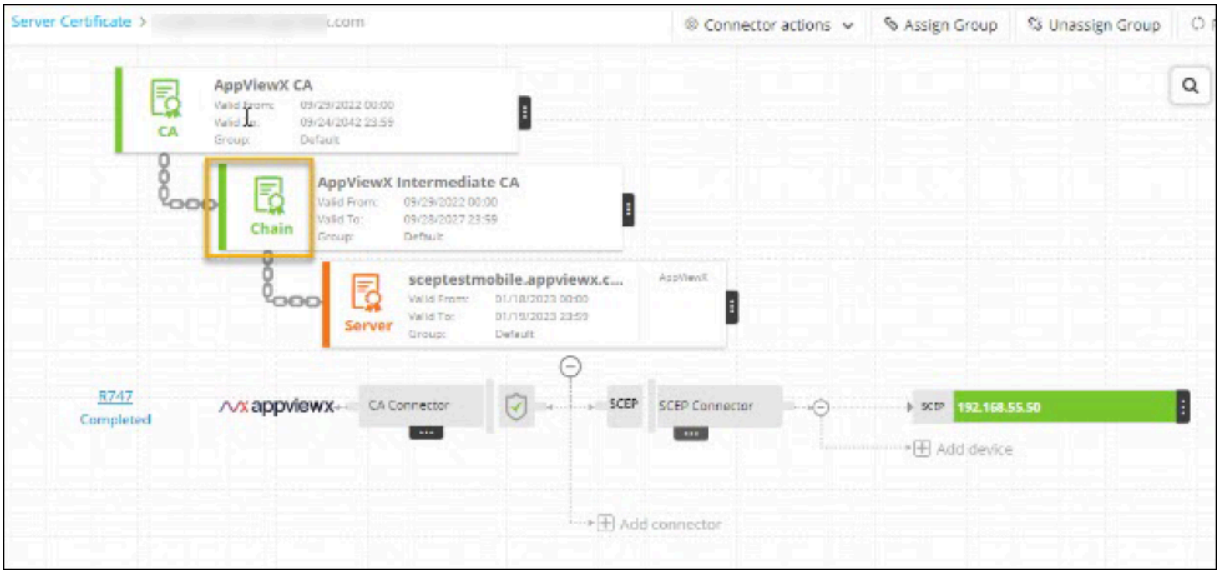
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



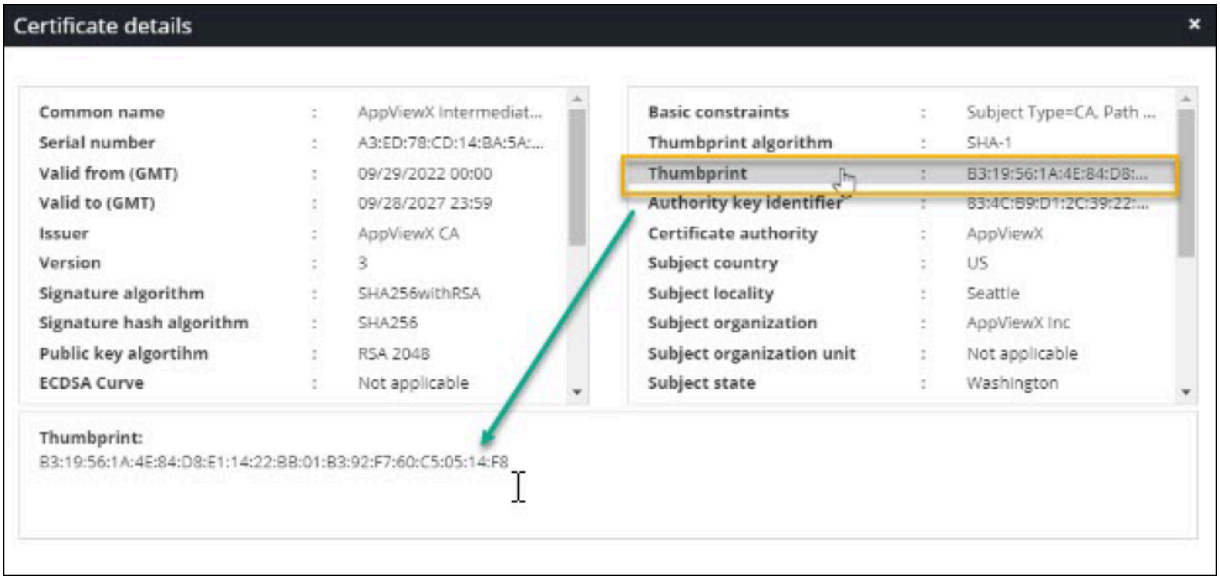
9. Click the **Details** tab and then select the Thumbprint field.
   The full value is displayed in the section below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. Copy this hex value and paste in the text pad. Use this value in the Fingerprint field in JAMF Pro (described in the section below).
    Consequently, another way to obtain the hex value without having to manually delete the colons in the thumbprint can is described below.
11. Execute steps 1 to 5 described above.



12. Click the Issuer certificate.

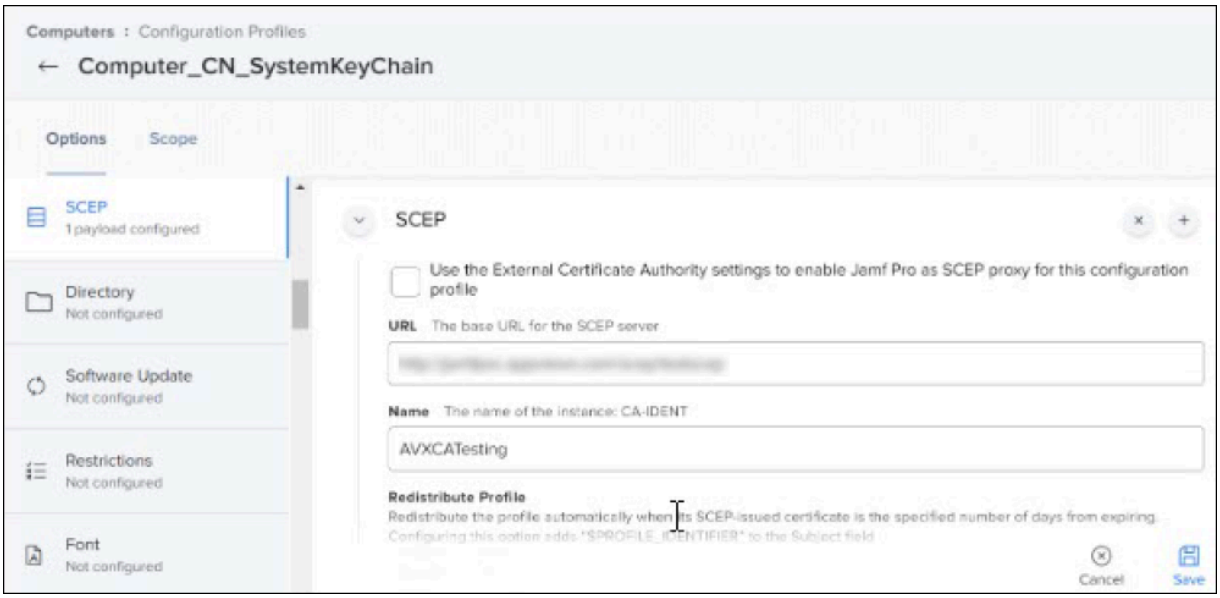


13. In the Certificate Details pop-up, click the **Thumbprint** value.
    The full value is displayed in the section below.
14. Copy this hex value and paste in the text pad. Ensure to remove all the colons before using it in the Fingerprint field in JAMF Pro (described in the section below).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

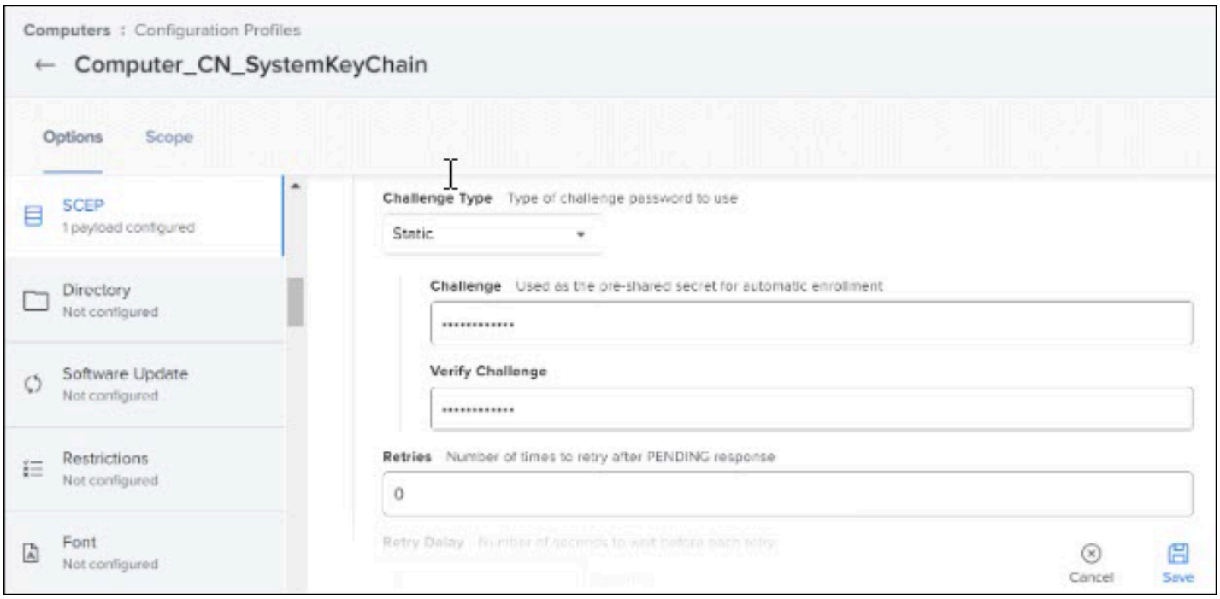
Configuring SCEP

1. Navigate to **SCEP Configuration Profiles** screen.



2. In the **URL** field, enter the AppViewX server's publicly exposed SCEP URL.
3. In the **Name** field, enter the desired name for this configuration.
4. From the **Redistribute Profile** dropdown, choose a value to specify the number of days before the certificate needs to be renewed. For example, if you want a certificate to be renewed 15 days before expiry, then set the **Redistribute Profile** to 15 days.
5. In the Subject field, enter the variable names. The $ (dollar) sign may be used with the variable name. Refer to the Mobile Device Configuration Profiles page to learn about the variable names supported in Jamf.
6. From the **Subject Alternative Name Type** dropdown, select *None*.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



7. From the Challenge Type dropdown, select the following:

   a. **Static** - If you want all computers and mobile devices to use the same challenge password, choose “Static” and specify a challenge password. The challenge password will be used as the pre-shared secret for automatic enrollment.

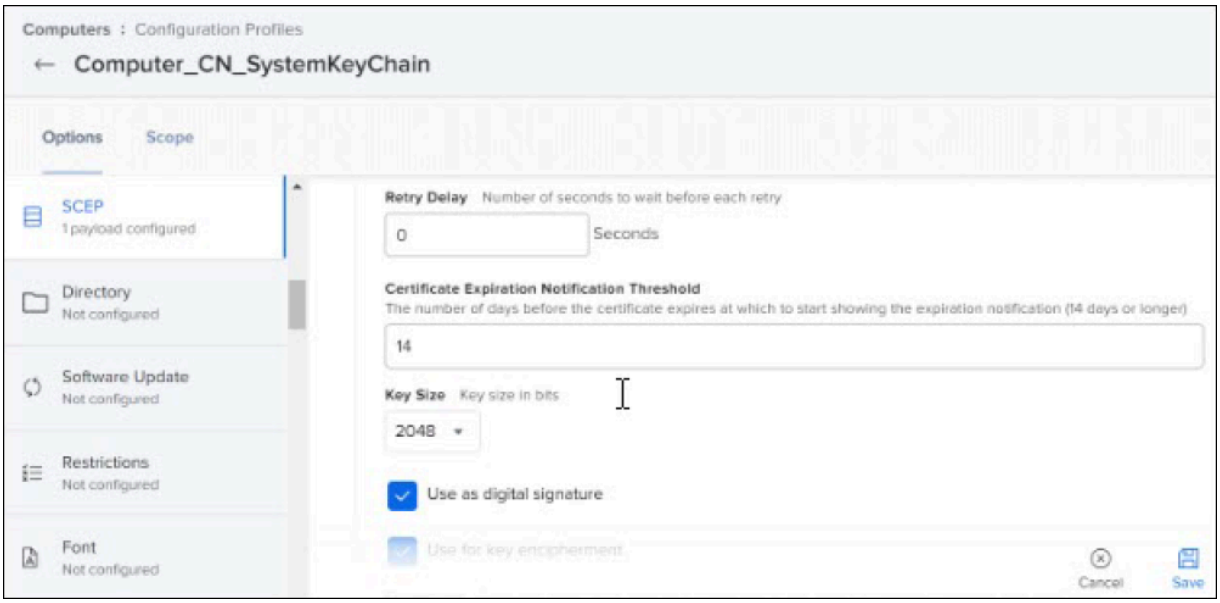
   b. **Dynamic** - If you are using a non-Microsoft CA and you want each computer and mobile device to use a unique challenge password, choose “Dynamic”. The Dynamic challenge type requires use of the Classic API and membership in the Jamf Developer Program. The Dynamic challenge uses the "Fingerprint" or "Thumbprint" to authenticate the user instead of a username and password. The Thumbprint hash value for the **Fingerprint** field in Jamf Pro can be found on the profile you receive. Before selecting this option, contact your Jamf account representative to learn more about the Jamf Developer Program and the additional steps you need to take to use this option.

   > **Note:** Currently, CERT+ does not support the dynamic challenge passphrase.

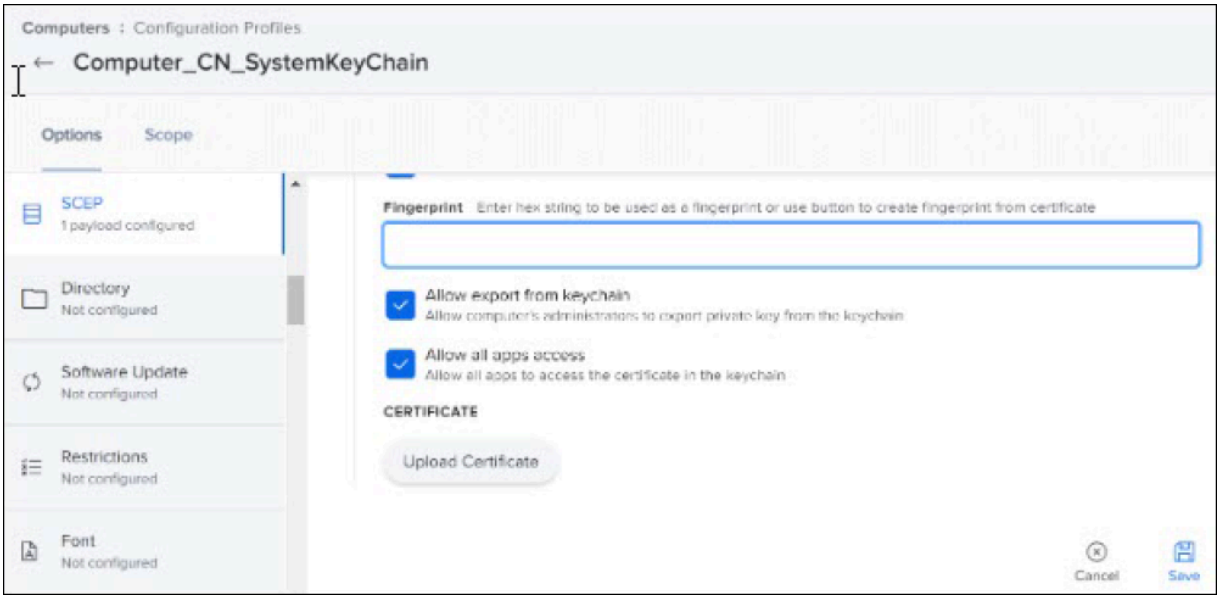
8. In the **Challenge** and **Verify Challenge** fields, enter the AppViewX SCEP Challenge Password configured in AppViewX SCEP UI.

> **Note:** This is a mandatory step. The Challenge password is mandatory while using this deployment model. The same challenge password set in the prerequisite should be configured in the JAMF.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

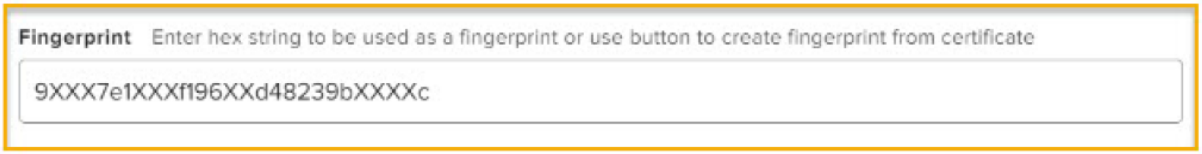


9. In the **Retry Delay** field, enter a desired value (in seconds).
10. In the **Certificate Expiration Notification Threshold** field, enter the number of days before the certificate expiration at which a notification will start displaying.
11. From the **Key Size** dropdown, select value *2048*.
12. Select the checkboxes **Use as digital signature** and **Use for key encipherment**.



13. In the **Fingerprint** field, enter the hex string to be used as a fingerprint.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

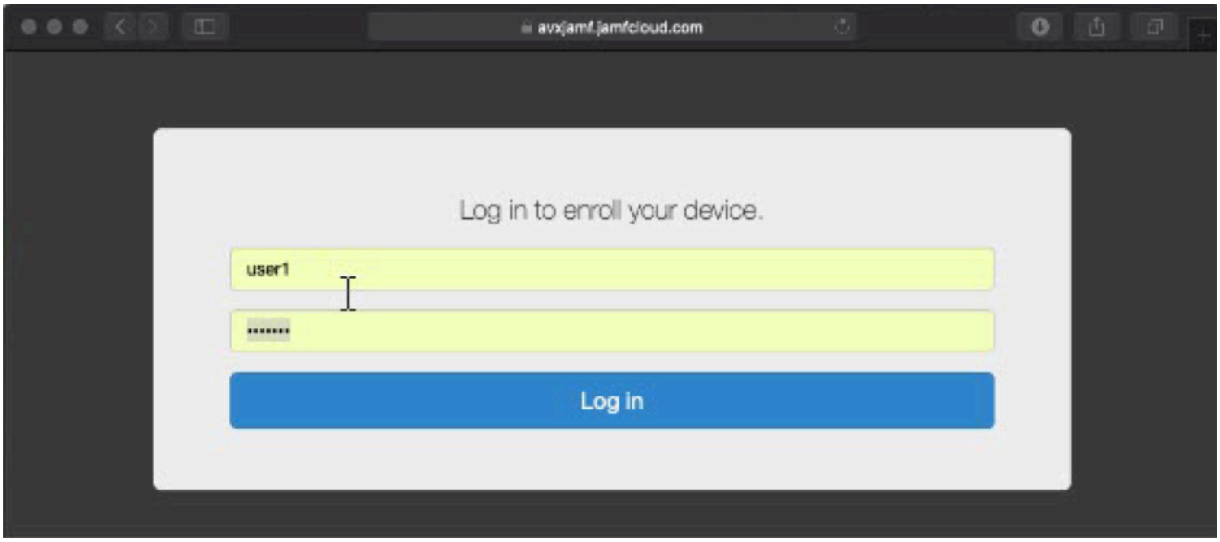


14. Select the checkboxes **Allow export from keychain** and **Allow all apps access**.
15. Click **Save**.

Initiating the Enrollment from a Device

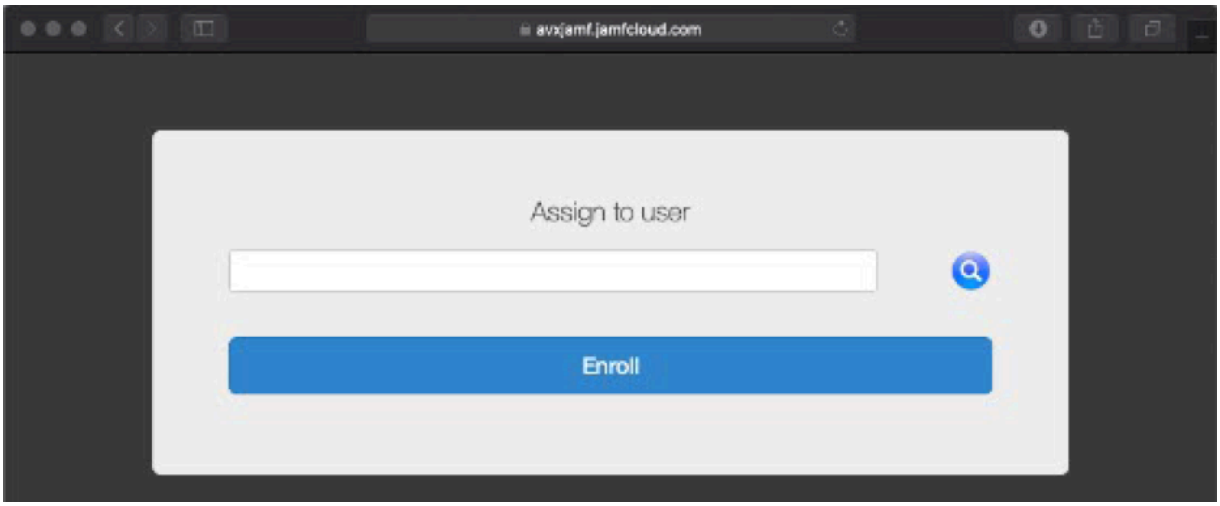
This section provides details of testing the Jamf cloud configuration performed in the previous section. It is recommended to open the JamfPro Enrollment URL using a Safari browser, as other browsers are not capable of identifying the received configuration profile and installation to the machine. Follow the instructions shown in the MacOS screen.

1. Enter the URL, for example - https://avxjamf.jamfcloud.com/enroll/ in the Safari browser.
2. Enter a valid username and password.

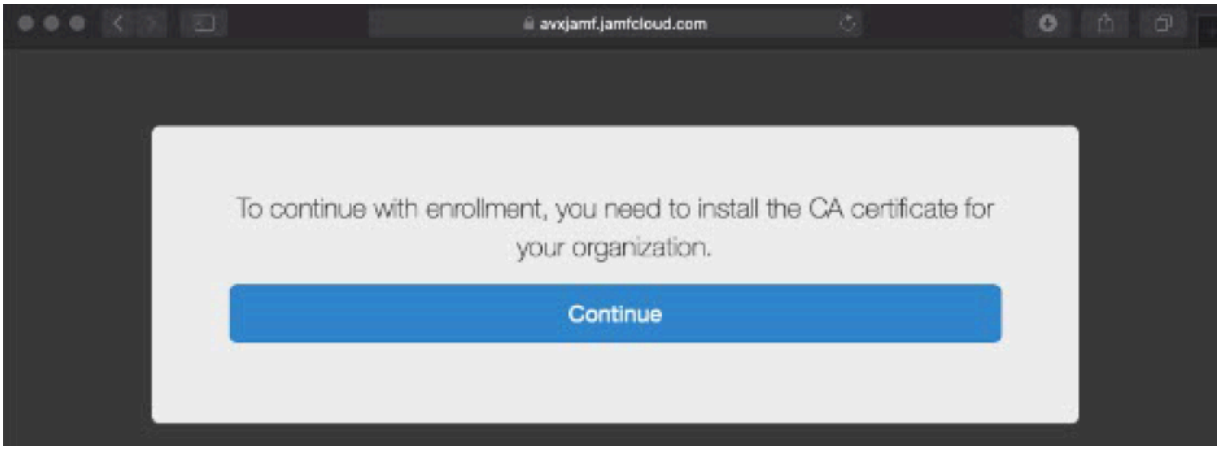


3. Leave the **Assign** to user field empty and click **Enroll**.

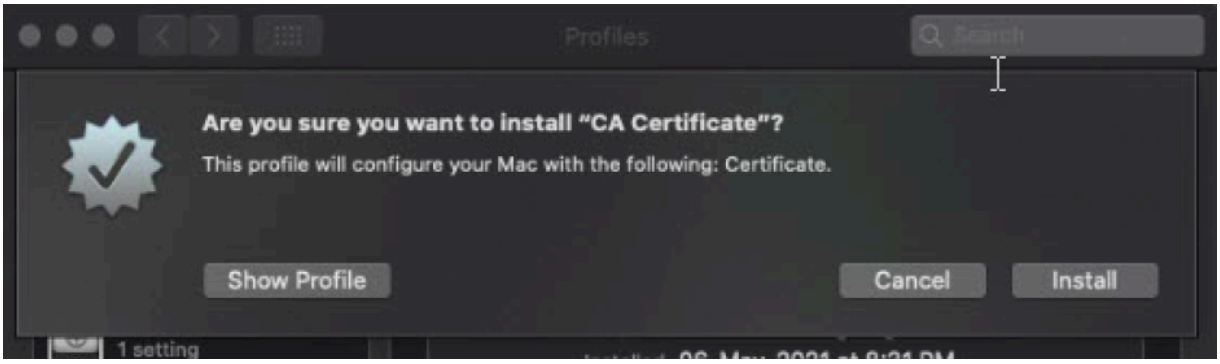
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. To continue with the enrollment (installation of CA certificate), click **Continue**.

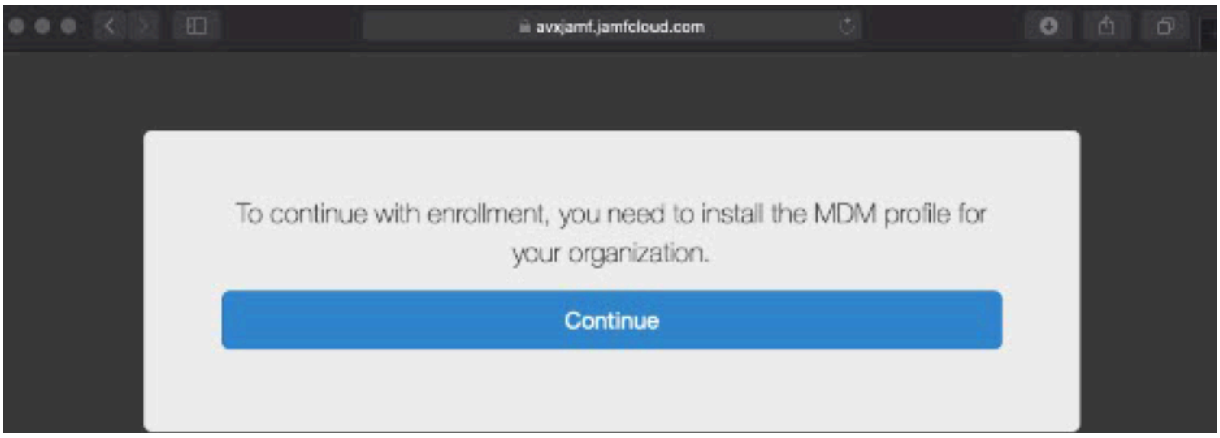


5. To confirm installation of the CA Certificate, click **Install**.

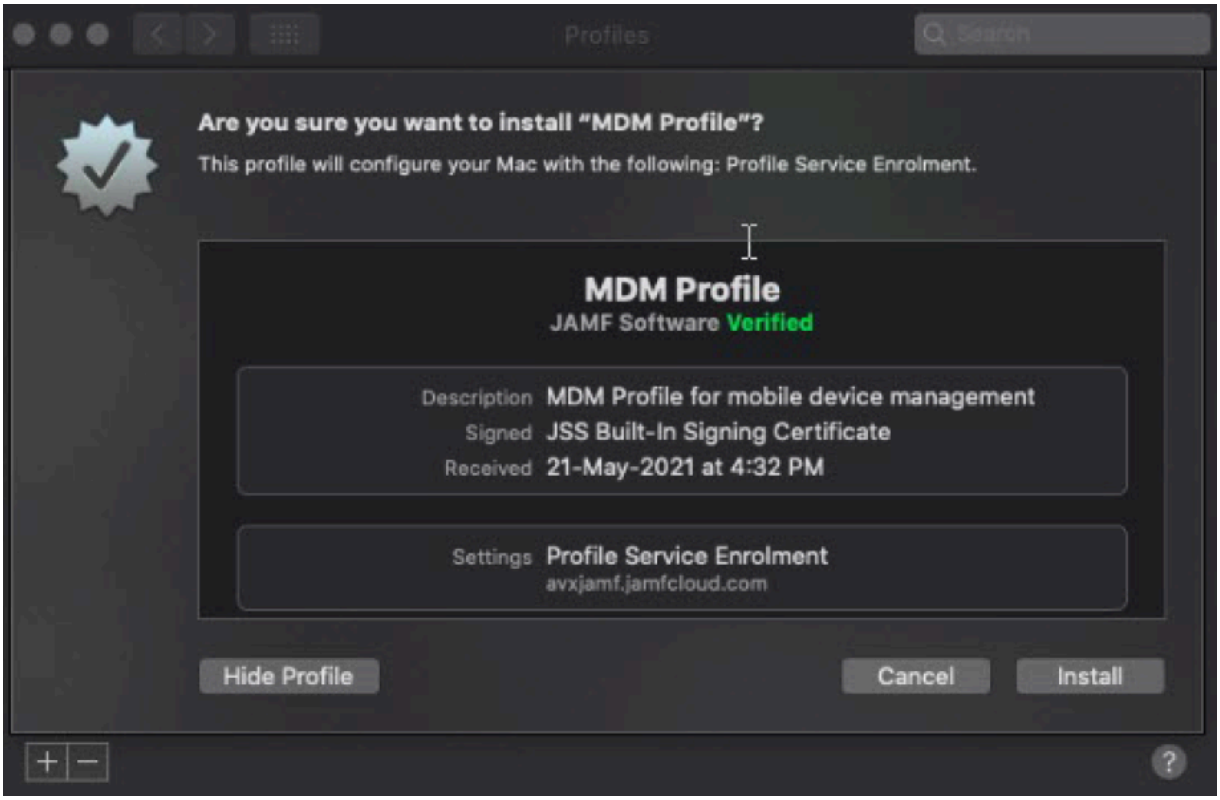


6. To continue with the enrollment (installation of the MDM profile), click **Continue**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



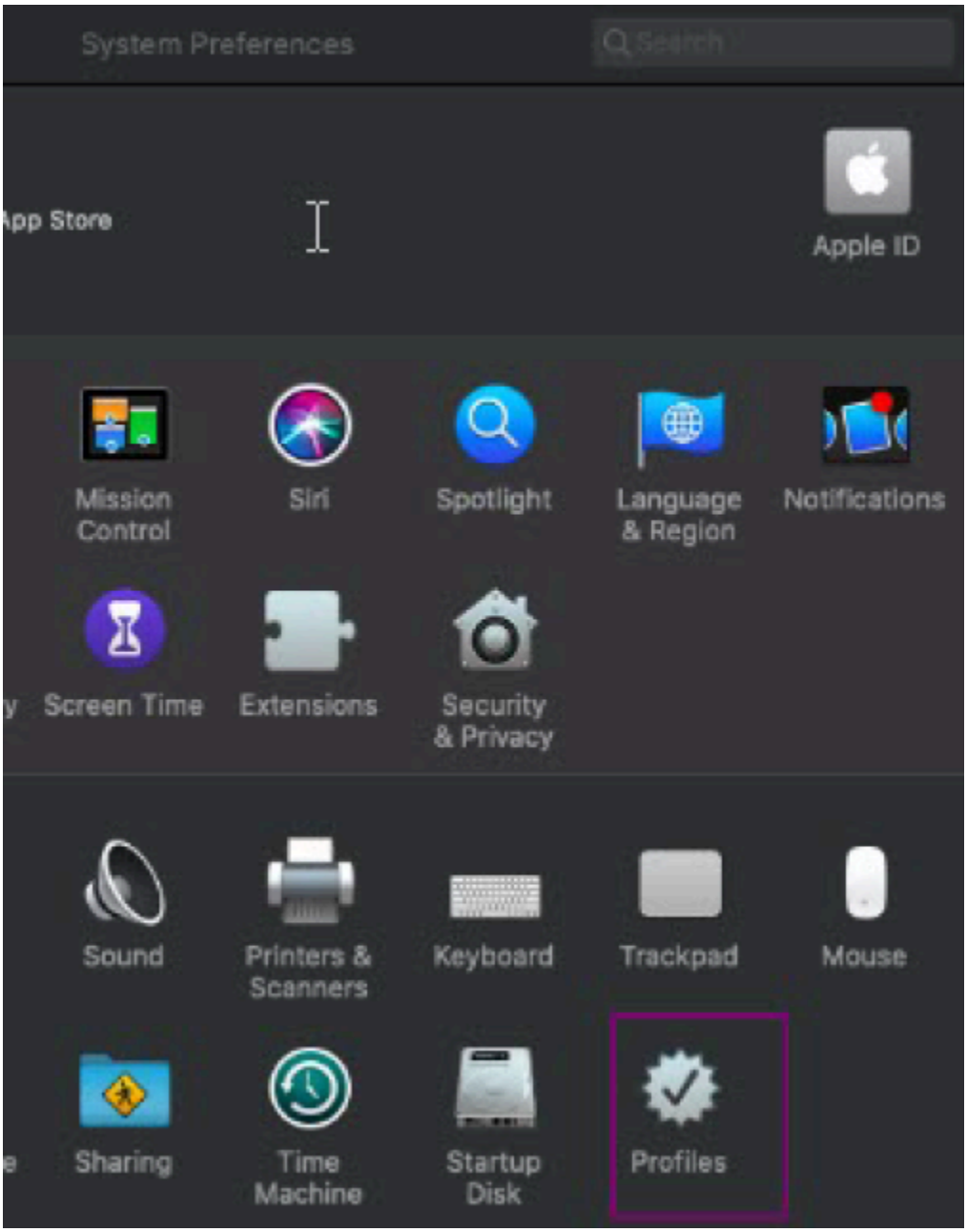
7. To confirm installation of the MDM Profile, click Install, and enter the valid credentials to carry out the installation.



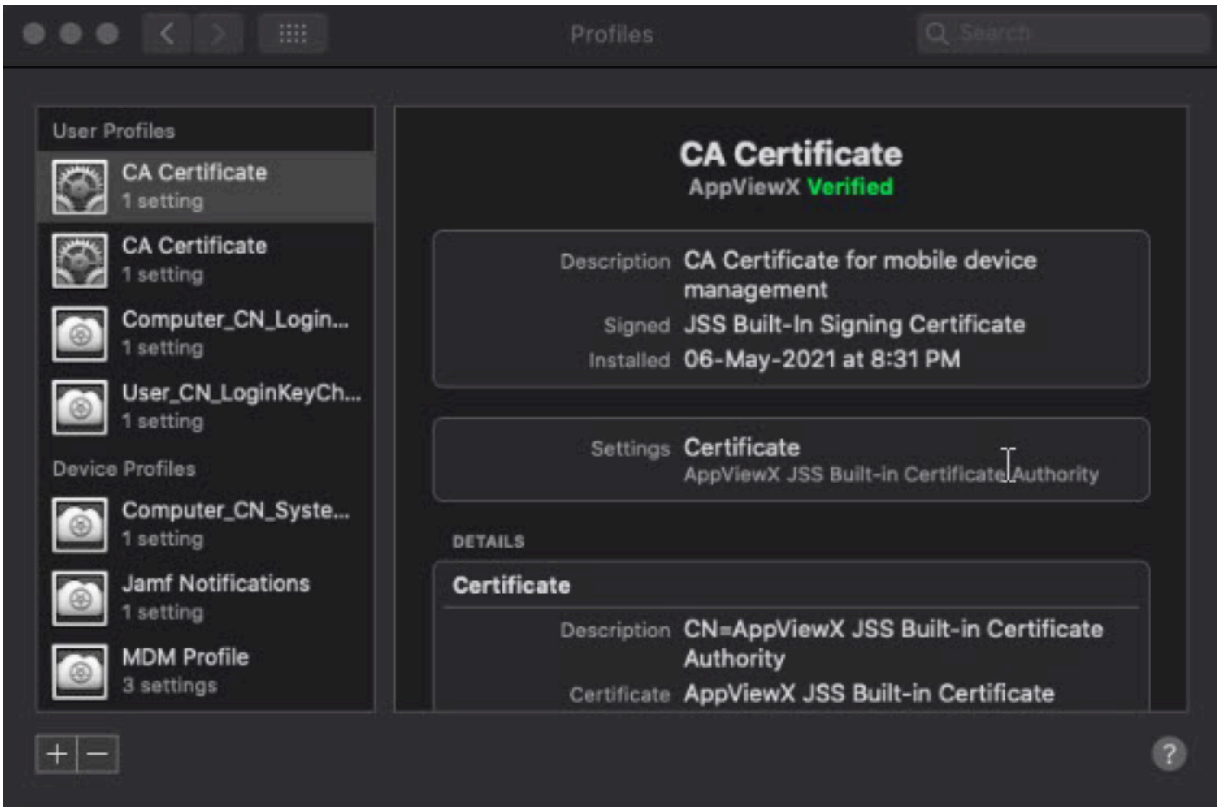
8. After the installation is complete, the following message is displayed – "The enrollment process is completed."
9. Wait for approximately one minute for the installation of the Profile and Certificate. (Profile contains SCEP configuration and during the installation process, the device directly sends a SCEP request to the AppVIewX Server.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. After the installation, the profiles can be verified by clicking **System Preferences** > **Profile**. All the installed profiles must be visible.



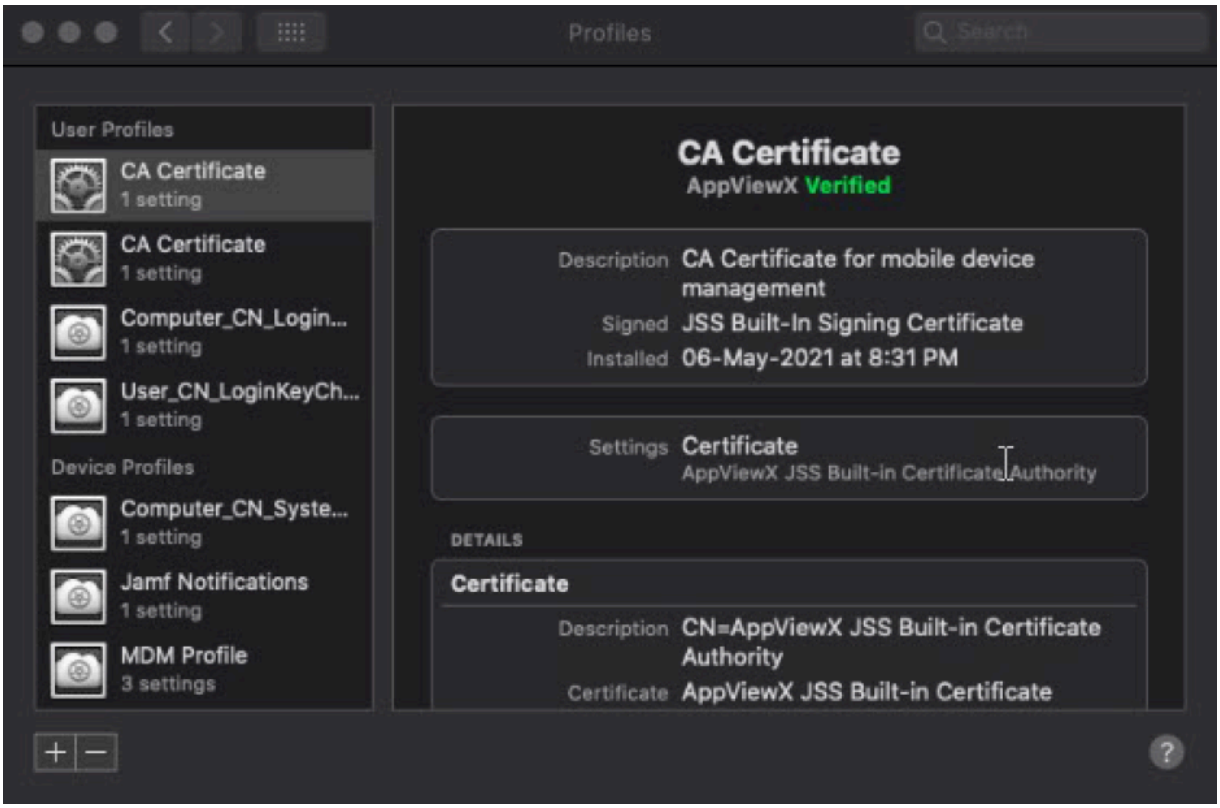
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



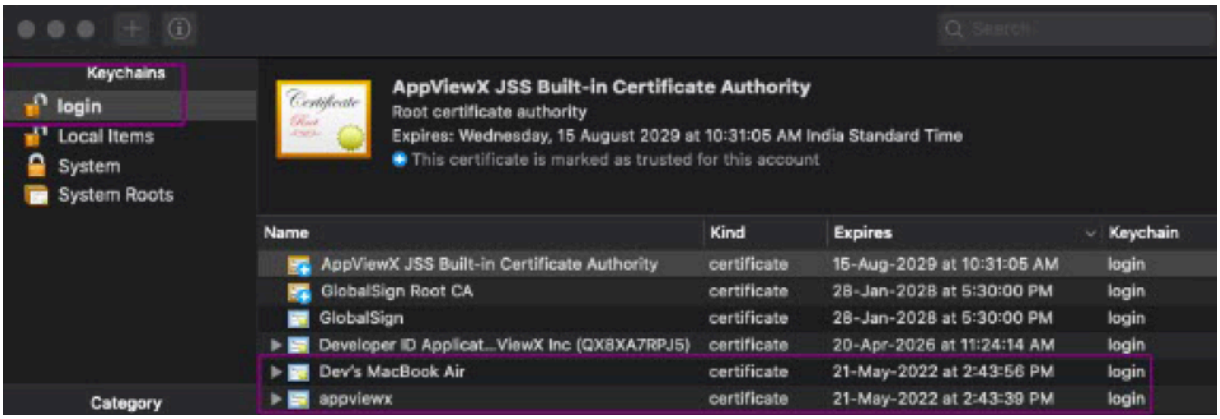
Note: Deleting the MDM profile deletes all the information from the Profiles. A fresh enroll may be tried later.

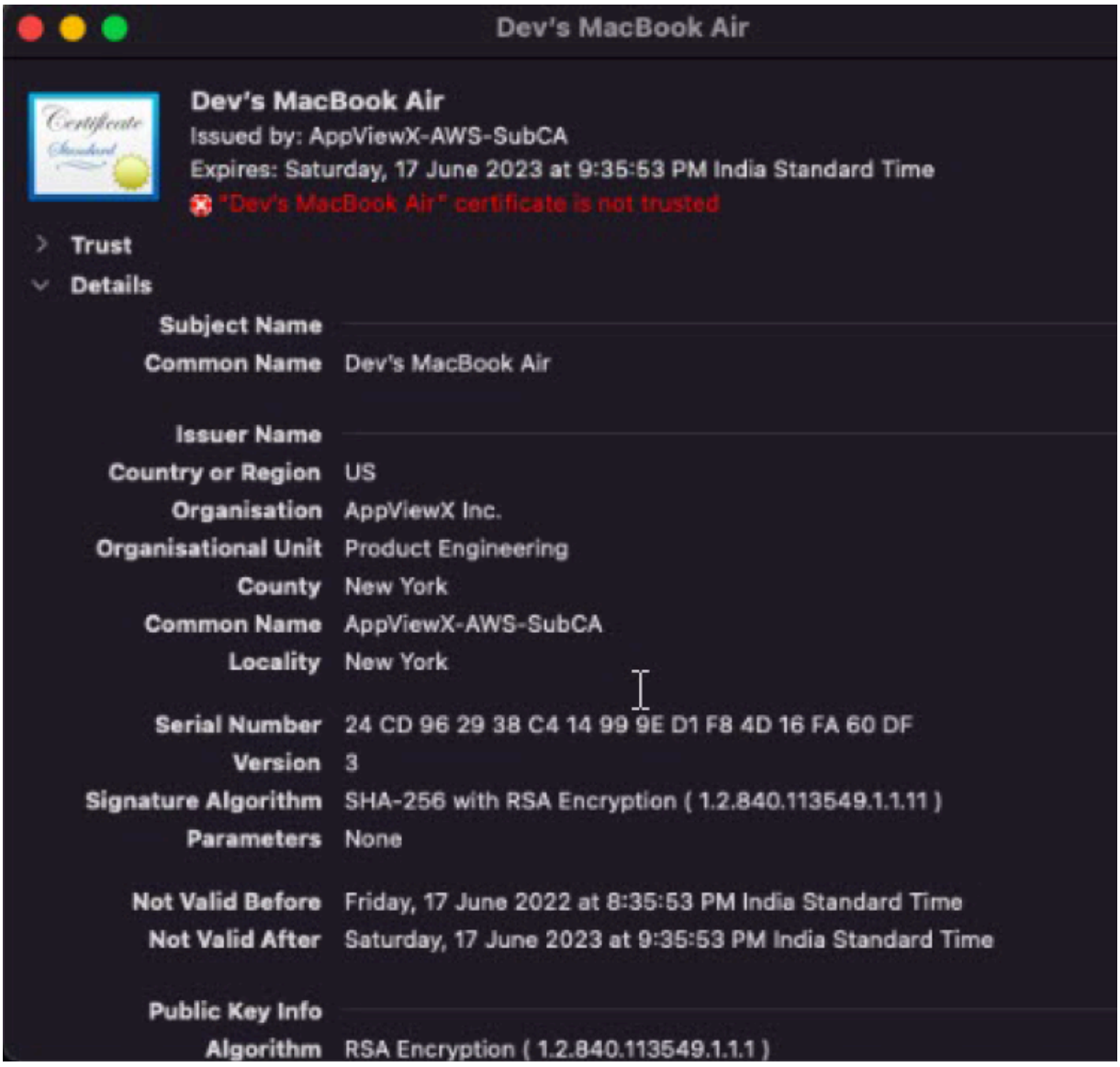
11. To verify the certificate, navigate to **Keychains** (User/System) and validate the certificates that were Installed for each configuration profiles with the respective CN Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

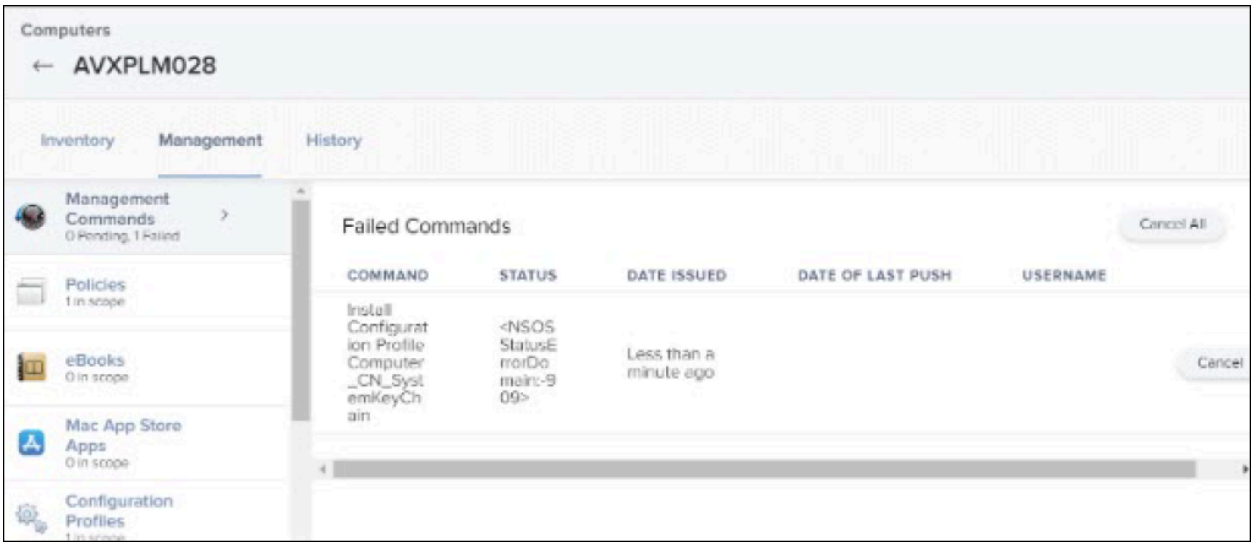




Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting

The failed commands or errors can be viewed here for troubleshooting.



References

#	Topic	URL
1	About Jamf	https://www.electric.ai/blog/jamf-ask-your-it-msp-for-it-by-name
2	Jamf Documentation	https://docs.jamf.com/10.42.0/jamf-pro/documentation/Jamf_Pro_Documentation.html
3	About SCEP	https://www.securew2.com/blog/simple-certificate-enrollment-protocol-scep-explained
4	Mobile Device Configuration Profiles	https://docs.jamf.com/10.30.0/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

What's Next

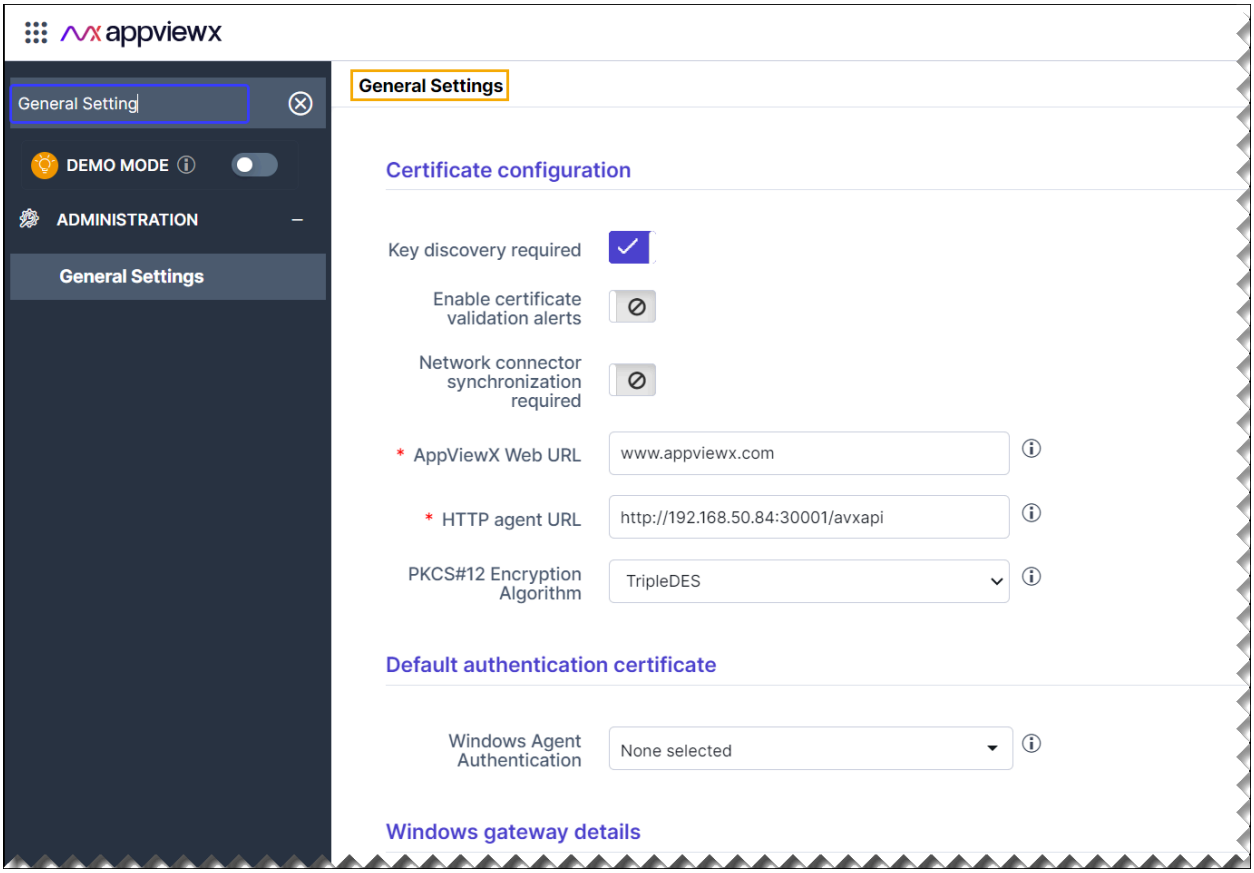
Refer to the following sections for auto-enrolling protocols:

- AppViewX Integration with Microsoft Intune Integration
- AppViewX Integration with SCEP
- EST Client Configuration Guide
- ACME Configuration Guide - Posh-ACME

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring General Settings

The **Certificate Configuration** section manages key discovery, certificate alerts, and external agent connection settings. The **Default Authentication Certificate** allows the selection of a certificate for authenticating Windows agents. The **Windows Gateway Details** configure interactions with Windows systems, specifying the gateway's name, URL, and a client authentication certificate. This page is crucial for ensuring secure communication between AppViewX CERT+ and external systems, enabling automated certificate management and secure key handling.



1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION**, and then click **General Settings**.
2. Select/Enable the **Certificate Configuration** parameters.

Field description for Certificate Configuration Section

Fields	Description
Key discovery required	**Default**: Enabled. If enabled (as shown), this setting requires the platform to perform key discovery. This means CERT+ will attempt to find private keys

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	associated with certificates when importing or managing certificates in the system.
Enable certificate validation alerts	**Default**: Disabled. If enabled, the system would notify administrators or users of issues like certificate validation failures, expired certificates, or other alert-worthy conditions related to certificates.
Network connector synchronization required	**Default**: Disabled. This setting, when enabled, ensures synchronization between the CERT + platform and external network connectors. It is useful for ensuring that the certificate data is consistent across networked systems.
***AppViewX Web URL**	This field contains the base URL for the **AppViewX** web interface (in this case, `www.appviewx.com`). This URL is used send the client certificate to email address specified during certificate creation.
***HTTP agent URL**	Specifies the URL for the **HTTP agent**. The URL shown here (for example: `https://pe-cert-ecosystem-xxx.abc.appviewx.net:xxxx/...`) is used to perform CRL check for AppViewX issued certificate.
PKCS#12 Encryption Algorithm	**Default**: TripleDES. In this case, the encryption algorithm selected is **Triple DES**. This option controls the algorithm used to encrypt PKCS#12 files, which are used to bundle private keys with certificates. The available options are: • **TripleDES** • **AES**.
**: Mandatory fields*	

3. Select the **Default authentication certificate** parameter.

Field description for Default authentication certificate Section

Field	Description
Windows Agent Authentication	**Default**: None Selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown allows the selection of a certificate for use with **Windows Agent Authentication**. This certificate would authenticate the Windows agent communicating with AppViewX, ensuring secure interactions.

4. Select the **Windows gateway details** parameters.

Field description for Windows gateway details Section

Field	Description
***Windows gateway name**	It is used to specify the name of the Windows gateway that the AppViewX CERT+ platform will communicate.
***Windows gateway URL**	It should contain the URL or IP address of the Windows gateway. The gateway facilitates communication between the AppViewX platform and Windows environments, such as for certificate distribution or renewal.
Client Authentication Certificate	**Default**: filename.pkcs The field shows an input box where a **.pkcs** file can be uploaded. This file would contain the client authentication certificate, which is used to securely authenticate the connection between AppViewX and the Windows gateway. The certificate helps establish secure communication between the two systems. The **Upload** button allows you to upload the <.pkcs> file containing the client certificate
**: Mandatory fields*	

5. Click **Add**.
6. Click **Save**.
7. To reset the selected/entered details, click **Reset**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Appendix A: Prerequisites for Enabling the Integrated Windows Gateway Mode

Refer to the following models for enabling the Integrated Windows Gateway mode.

- Privlilege model (For IIS devices)
- Minimum privilege model (CA and Devices other than IIS)

Privlilege Model (For IIS devices)

Usecases	Required	Level	Type	Details	Purpose
Device and CA communications	User account type	User	User Account	Added to Group 1. Domain Admin	To ensure seamless WinRM communication from a remote Java process, adding the user to the Domain Admin group is necessary. This grants the required permissions for enabling communication, remote execution,preventing operational failures and maintaining functionality.
				2. Remote Management Users	Adding the user to the Remote Management Users group is essential for enabling WinRM communication, as it grants the necessary permissions for remote execution and management tasks, ensuring secure and efficient operation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Privlilege Model (For IIS devices) (continued)

Usecases	Required	Level	Type	Details	Purpose

	User permission	System	Winrm Permissions	To enable WinRM communication in a Windows machine, follow the instructions given below:
				
				The following steps must be executed manually:
				
				1. **Enabling PSRemoting:**
				`Enable-PSRemoting -Force`
				2. **Configure WinRM service:**
				`Set-Service -Name WinRM -StartupType Automatic`
				`Start-Service -Name WinRM`
				3. **Allow WinRM through Firewall (if any):**
				`Enable-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC"`
				`Enable-NetFirewallRule -Name "WINRM-HTTP-In-TCP-DOMAIN"`
				4. **Permissions for WSMAN:**
					The WinRM methodology is used to connect Windows machines with the Cloud Connector, using PowerShell scripts and commands for executing actions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Privlilege Model (For IIS devices) (continued)

Usecases	Required	Level	Type	Details	Purpose
				winrm set winrm/config/service '@{AllowUnencrypted="true"}' winrm set winrm/config/service/auth '@{Basic="true"}'	
	Ports	System	5985	This port should be enabled and open for communication from CC	
		System	5986	For HTTPS communication, end devices should be enabled with HTTPS specific configuration (not certified yet). To enable HTTPS for a Cloud Connector configuration, add the following properties in the **<CC Installation Path>/deps/properties/appviewx.properties** file: WINRM_HTTPS_PORT=5986 WINRM_HTTPS_ENABLED=true	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Privlilege Model (For IIS devices) (continued)

Usecases	Required	Level	Type	Details	Purpose
				Note: Once WINRM with HTTPS is enabled for a Cloud Connector, all communications between the Cloud Connector and any Windows machine will happen exclusively over HTTPS. To enable HTTPS for a Windows machine, refer the **EnableHTTPs.ps1** script below.	

Minimum Privilege Model (CA and Devices other than IIS)

Usecases	Level	Type	Details
Device and CA communications (Other than IIS devices and management)	User account	service Account	A basic service account to communicate with Windows devices..
	User permission	Winrm Permissions	All these steps can be done by executing **UserPrivEnablement.ps1** script given below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Minimum Privilege Model (CA and Devices other than IIS) (continued)

Usecases	Level	Type	Details

			The following commands are executed as part of the **UserPrivEnablement.ps1** script.
			
			1. **Enable Auth:**
			`winrm set winrm/config/service/Auth '@{Basic="true"}'`
			2. **User group requirements:** Should be added to below groups
			a. Remote Management Users
			b. Performance Monitor Users
			c. WinRMRemoteWMIUsers (This Group should be created if not present)
			3. In a CMD Window (run as Administrator) execute
			`winrm configSDDL default`
			Add the **desired user** and configure permissions. Check 'Allow' for Read (Get, Enumerate, Subscribe) and Execute (Invoke)

Fetch CA - Command execution host	Device type	Domain controller (Primary)	Devices that are part of domain controllers gets all CA's available in that domain. Use the command to check the same: `systeminfo | findstr /C:"OS Configuration` The Device can either be domain controller or the device that responds with the CA templates for the command below:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Minimum Privilege Model (CA and Devices other than IIS) (continued)

Usecases	Level	Type	Details
			winrs -r:localhost -u:<username> -p:<password> powershell . "certutil -config "<CA_Server\CA_Name>" -caTemplates -v" *Sample command*: winrs -r:localhost -u:user1 -p:pass powershell . "certutil -config "TestCAServer.test.com\TestCaServer-001>" -caTemplates -v"
Ports	Winrm with HTTP	5985	This port should be enabled and open for communication from CC
	Winrm with HTTPS	5986	For HTTPS communication, end devices should be enabled with HTTPS specific configuration (not certified yet). To enable HTTPS for a Cloud Connector configuration, add the following properties in the **<CC Installation Path>/deps/properties/appviewx.properties** file: WINRM_HTTPS_PORT=5986 WINRM_HTTPS_ENABLED=true **Note:** Once WINRM with HTTPS is enabled for a Cloud Connector, all communications between the Cloud Connector and any Windows machine will happen exclusively over HTTPS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Minimum Privilege Model (CA and Devices other than IIS) (continued)

Usecases	Level	Type	Details
			To enable HTTPS for a Windows machine, refer the **EnableHTTPs.ps1** script below.

Script: **UserPrivEnablement.ps1**

```
# Get the username at runtime
$user = Read-Host "Enter the username"

# 1. Enable Authentication for WinRM
winrm set winrm/config/service/Auth '@{Basic="true"}'

# 2. Add the user to required local groups
net localgroup "Remote Management Users" /add $user
net localgroup "Performance Monitor Users" /add $user

# Check if "WinRMRemoteWMIUsers__" exists, if not create it
$groupName = "WinRMRemoteWMIUsers__"
$groupExists = Get-LocalGroup -Name $groupName -ErrorAction SilentlyContinue

if (-not $groupExists) {
    New-LocalGroup -Name $groupName -Description "WinRM Remote WMI Users"
}

# Add the user to the "WinRMRemoteWMIUsers__" group
Add-LocalGroupMember -Group $groupName -Member $user

# 3. Execute the 'winrm configSDDL default' command to configure permissions
Invoke-Expression -Command "cmd /c 'winrm configSDDL default'"

# Set permissions for the user (e.g., Read and Execute)
# Note: You would typically do this in the "winrm configSDDL default" command manually or via script
# to allow Read (Get, Enumerate, Subscribe) and Execute (Invoke) for the specific user, but this may require elevated permissions.

# 4. Update Group Policy
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
gpupdate /force


Write-Host "User account setup complete. Please check the permissions in the WinRM configuration if needed."
```

Script: **EnableHTTPs.ps1**

```
# Prompt user for the certificate thumbprint
$newCertThumbprint = Read-Host "Enter the new certificate thumbprint"


# Keep asking for the IP address until it is not empty
$ip = ""
while (-not $ip) {
    $ip = Read-Host "Enter the IP address (this cannot be empty)"
    if (-not $ip) {
        Write-Host "IP address cannot be empty. Please enter a valid IP address."
    }
}


$port = "5986"  # Default port is always 5986
$ipport = $ip+":"+$port  # Combine IP and port into one variable
$hostname = ([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname


# Show the existing certificate thumbprint associated with the WinRM HTTPS listener
$currentBinding = netsh http show sslcert ipport=$ipport


if ($currentBinding -like "*Certificate Hash*") {
    $currentCertThumbprint = ($currentBinding | Select-String -Pattern "Certificate Hash" | ForEach-Object { $_.Line.Split(':')[1].Trim() })
    Write-Host "Current certificate thumbprint: $currentCertThumbprint"
} else {
    Write-Host "No existing certificate bound to port: $port"
}


# Disassociate the existing certificate if a thumbprint is found
if ($currentCertThumbprint) {
    netsh http delete sslcert ipport=$ipport


    # Verify deletion
    $postDeleteBinding = netsh http show sslcert ipport=$ipport
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    if ($postDeleteBinding -like "*The system cannot find the file specified*") {
        Write-Host "Successfully removed the certificate binding from port $port"
    } else {
        Write-Host "Failed to remove the certificate binding. Exiting."
        exit 1
    }
} else {
    Write-Host "No certificate found to disassociate."
}

# Delete the existing WinRM HTTPS listener
Write-Host "Deleting the existing WinRM HTTPS listener..."
winrm delete winrm/config/Listener?Address=*+Transport=HTTPS

# Add the new thumbprint to the WinRM config
Write-Host "Setting the new certificate thumbprint in WinRM configuration..."
winrm set winrm/config/service "@{CertificateThumbprint=`"$newCertThumbprint`"}"

# Create a new listener and associate the new certificate with the specified port
Write-Host "Creating a new listener and binding the new certificate to port $port..."
$appId = [guid]::NewGuid().ToString()  # Generate a random app GUID
netsh http add sslcert ipport=$ipport certhash=$newCertThumbprint appid="{$appId}"

# Create the new listener using WinRM
New-Item -Path WSMan:\Localhost\Listener -Transport HTTPS -Address * -CertificateThumbprint $newCertThumbprint -HostName $hostname -Force

# Verify the new binding
$finalBinding = netsh http show sslcert ipport=$ipport
if ($finalBinding -like "*Certificate Hash*") {
    Write-Host "New certificate bound to port $port successfully."
} else {
    Write-Host "Failed to associate the new certificate."
    exit 1
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Appendix B: List of Scheduled Jobs

Note: To avoid queue overload when there are a large number of devices/multiple requests sent to the queue simultaneously, a delay has to be introduced for triggering the **Device and Certificate synchronization** and **Device Server Status Synchronization** jobs from the job scheduler at 12 AM and 3 AM.

To implement this, add a custom delay value in the cert_metadata collection. Following is a sample that configures a delay of 60 seconds:

```
Unset
{
"_id": "MISC_SYNC_QUEUE_DELAY_IN_SEC",
"constant": "60"
}
```

Currently, the discovery/config-sync calls for all devices are triggered in order, without any delay. With the delay configured, when the specified jobs are triggered, the discovery/config sync call for each device will be triggered after the pre-defined interval.

Auto Regenerate Certificates

This job is triggered periodically to check whether the regeneration action to be triggered for the certificates in the inventory that are enabled with Regenerate Automatically in the CA connector, based on whether the certificate is reached the time to trigger the regenerate action.

- **Check** - The cron job is executed for auto regeneration of certificates at a scheduled time.
- **Monitor** - The scheduled job is monitored and triggered by default daily at 02:00:00 A.M.

Note: Auto generates for the certificate available in the inventory, enabled with Auto regenerate action in the CA connector when the threshold is reached, as mentioned in the CA connector form, the auto regenerate will be triggered.

- **Audit** - The internal business logic of auto-regenerates certificates is captured via audit logs and notification logs in the logging module.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Automated Credential Rotation

This job automates the rotation of credentials (keys, passwords, or tokens) for integrated systems or devices. It can be scheduled to run at regular intervals based on the credential's TTL, or triggered on demand. The job is disabled by default and can be enabled as needed.

For instructions on enabling/disabling and configuring the job, see Working with the Job Scheduler.

Auto-Renew Certificates

This job is triggered periodically to check whether the renewed action to be triggered for the certificates in the inventory that are enabled with Renew Automatically in the CA connector, based on a certificate is reached the time to trigger the renew action.

- **Check** - To auto-renew certificates if it is scheduled.
- **Monitor** - The scheduled job is monitored and triggered by default daily every 6 hours.
- **Audit** - The internal business logic of auto-renew certificates is captured via audit logs and notification logs in the logging module.

CA Connector Validity Updater

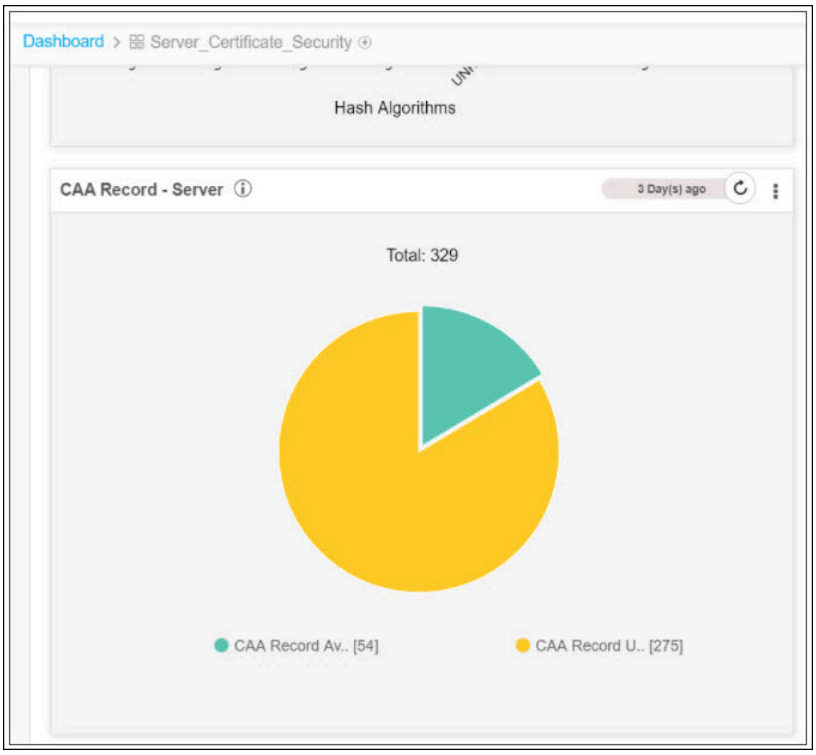
It allows to check the validity offered by CA and update the same in CA connector and policy.

- **Check** - The cron job is executed to check the validity offered by the External CA and update the same in CA connector and Certificate policy.
- **Monitor** - The scheduled job is monitored and triggered by default on every Sunday at 06:00:00 A.M.
- **Audit** - The internal business logic to update the CA connector and Policy is captured via audit logs and notification logs in the logging module.

Certificate CAA Record Check

A Certification Authority Authorization (CAA) record is used to specify which certificate authorities (CAs) are allowed to issue certificates for a domain.CAA records allow domain owners to declare which certificate authorities are allowed to issue a certificate for a domain. They also provide a means of indicating notification rules in case someone requests a certificate from an unauthorized certificate authority. If no CAA record is present, any CA is allowed to issue a certificate for the domain. If a CAA record is present, only the CAs listed in the record(s) are allowed to issue certificates for that hostname.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- **Check** -
  - The cron job is executed to check the CAA record for all the certificates in the inventory.
  - Once the job is completed, the CAA report is updated in the server_certificate_security dashboard.
- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Monday.
- **Audit** - The internal business logic to check the CAA records for all the certificates are captured through audit logs and notification logs in the logging module.

Certificate Compliance Check

A compliance check is the process of review and analysis of the implemented controls to check that the implemented controls and their outputs meet the certificate policy requirements. It checks the compliance for all the certificates in the inventory. If the policy is changed the compliance will be in pending status till this job is executed.

- **Check**
  - The cron job is executed to check the compliance status for all certificates in the inventory.
  - If the policy is changed the compliance will be in pending status till this job is executed.
  - Once the job is completed, the **compliance report** is updated in the **server and client** certificates dashboard.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Monitor** - The scheduled job is monitored and triggered by default daily at 05:00 A.M.
- **Audit** - The internal business logic for compliance checks is captured via audit logs and notification logs.

Certificate Expiry Status Check

This job is triggered periodically to update the expiry status for all the certificates in the inventory.

- **Check** - The cron job is executed to check the expiry status of all the certificates available in the inventory.
- **Monitor** - The scheduled job is monitored and triggered by default daily 20 minutes every 5 hours.
- **Audit** - The internal business logic to check the expiry status is captured via audit logs and notification logs in the logging module.

Certificate Polling Request

This job gets triggered only during the performance of CLM actions. Once the CSR gets submitted to the Certificate Authority, until the signed certificate is received from the certificate authority, the polling request job gets triggered to collect the certificate in the response.

Certificate Revoke Status Check From CA

For all the certificates managed or monitored in the inventory, this job will be performed periodically at the configured duration. Based on this check, the certificate status in the inventory will be updated with either revoked or others.

Note: This feature is supported only for Digicert CA.

- **Check** - The cron job is executed to check only the certificate revoke status from the CA Portal.
- **Monitor** - The scheduled job is monitored and triggered by default every 15 minutes.
- **Audit** - The internal business logic to check the certificate revoke status from the CA portal is captured via audit logs and notification logs in the logging module.

Certificate Transparency Check

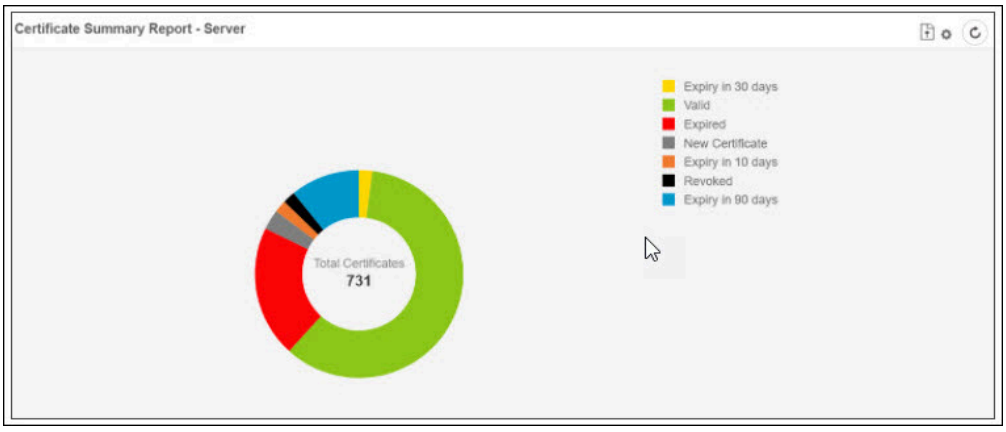
This is a periodical running job to update the certificate transparency report data available in the dashboard Server certificate security. It allows checking the certificate transparency for all certificates in the inventory (Google CT project). The Certificate Transparency safeguards the certificate issuance process by monitoring and auditing HTTPS certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Check**
  - The cron job is executed to check the Certificate transparency for all certificates in the inventory.
  - The internal business logic uses the Google CT project (Open source) to identify the violation
  - Once the job is completed, the CT and CAA reports are updated in the server_certificate_security dashboard.
- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Sunday.
- **Audit** - The internal business logic to check the CT for all the certificates is captured via audit logs and notification logs in the logging module.

Certificate Validation Check

This is a periodical running job to validate the chain of trust information for all the certificates in the inventory. Based on this validation, the certificate validation report will be updated with the latest data in the server certificate dashboard.



- **Check**
  - The cron job is executed to check the validation for all certificates in the inventory.
  - Once the job is completed, the certificate summary report is updated in the Server Certificate and Client Certificate Dashboard.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Monday.
- **Audit** - The internal business logic to check the CT for all the certificates is captured through audit logs and notification logs in the logging module.

Certificate Vulnerability Check

This is a periodical running job to update the vulnerability report data available in the dashboards Server endpoint security. It allows checking the vulnerability in the device such as Toodles, Heart bleed, and Roca.

- **Check** -
  - The cron job is executed to check the certificates and their device association
  - There is internal business logic to check the Poodle, Heart bleed, and Roca vulnerabilities for the associated device.
  - Once the job is completed the “Vulnerability reports” are updated in “Server_Endpoint_Security”, “Client_Endpoint_Security”.
  - The ROCA vulnerability is a cryptographic weakness that allows the private key of a key pair to be recovered from the public key in keys generated by devices with the vulnerability.
  - The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
  - The Poodle vulnerability lets an attacker eavesdrop on communication encrypted using SSLv3. The vulnerability is no longer present in the Transport Layer Security protocol (TLS), which is the successor to Secure Socket Layer (SSL).
- **Monitor** - The scheduled job is monitored and triggered by default weekly, on Saturday.
- **Audit** - The internal business logic to check the vulnerability of the device. It is captured via audit logs and notification logs in the logging module.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CRL Certificate Revocation Check

To download the CRL for all the certificates in the inventory and validate with the downloaded CRL record. You can change the revocation status in the inventory.

- **Check**
  - The cron job is executed to download CRL data for all the certificates available in the inventory.
  - Once CRL is downloaded compare and change the revocation status in the inventory.
- **Monitor** - The scheduled job is monitored and triggered by default daily every 6 hours.
- **Audit** - The internal business logic for certificate revocation check is captured via audit logs and notification logs in the logging module.

CRL Download Monitor Job

To monitor the certificates in inventory and download the CRL for the newly added certificate. Make sure that the below actions are completed for the CRL download monitor job.

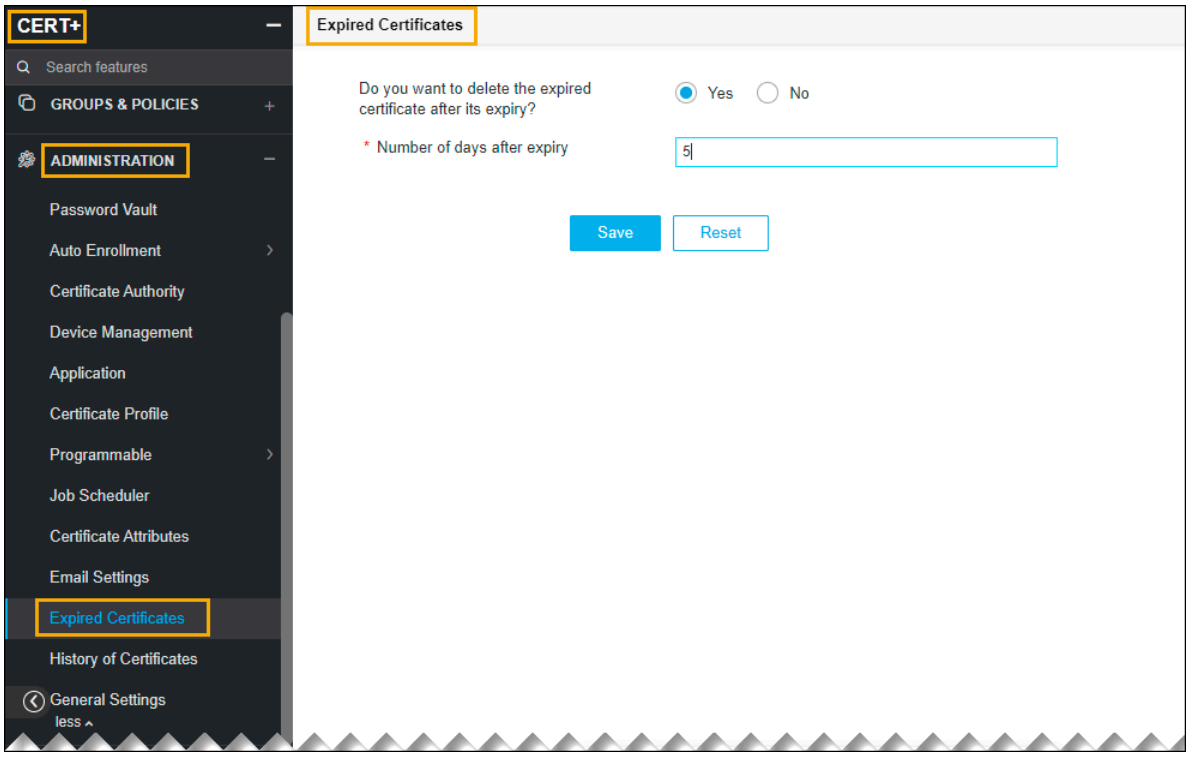
- **Check** - The cron job is executed to monitor the certificates in inventory to download the CRL for the newly synchronized certificate.
- **Monitor** - The scheduled job is monitored and triggered by default every 5 minutes.
- **Audit** - The internal business logic for the certificate download monitor job is captured via audit logs and notification logs in the logging module.

Delete Expired Certificates

This is a periodical job to check and delete the expired certificates available in the inventory. This job will be triggered only when this action is enabled in **Expired Certificates**.

- **Check** - The cron job is executed to delete the expired certificates in the inventory. To enable the delete expiry certificate function, do the following steps:
  1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Expired Certificates**.
  2. Enable **Yes** to delete the expired certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Note: Once enabled, automatically the expiry certificate will be deleted.

- **Monitor** - The scheduled job is monitored and triggered by default daily at 03:00:00 A.M.
- **Audit** - The internal business logic of auto regenerate certificates are captured via audit logs and notification logs in the logging module.

Device and Certificate synchronization

This periodical running job synchronizes the data such as certificates and objects used for application connectors from devices to AppViewX. The device includes ADC, Servers, Firewall, WAF, Cloud, and MDM.

- **Check**
  - The cron job is executed to synchronize the inventory certificates from the managed device inventory.
  - The device inventory is categorized as ADC, Server, WAF, Firewall, Cloud, MDM, and so on.
  - The job discovers all devices in the managed state.
- **Monitor**

Periodic CRL Update for AppViewX and Custom CAs

To do the CRL rotation for AppViewX and Custom CA. The CRL is regenerated, any expired certificates are removed from the CRL.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Check** - The cron job is executed to rotate CRL for AppViewX and Custom CA so that the CRL is regenerated, any expired certificates are removed from the CRL.
- **Monitor** - The scheduled job is monitored and triggered by default daily at 05:00:00 A.M.
- **Audit** - The internal business logic to update the CRL is captured through audit logs and notification logs in the logging module.

Working with the Job Scheduler

This topic describes the basic functionality of the job schedulers available in CERT+. These cron jobs are scheduled in the background to check, monitor, audit the certificates in inventory. The AppViewX Platform cron job checks the certificate cron job every 15 minutes and looks for the changes and triggers the job at a scheduled time.

The Cron job frameworks are:

- Check
- Monitor
- Audit

Check

- Each Cron Job is executed for the batch of certificates (depending on the job) asynchronously and on successful completion, the status is updated in the database.
- All Cron jobs executed asynchronously based on the scheduled time.
- Each Cron job is bound to the internal business logic to update the status in the database.

Monitor

- Cron jobs are scheduled at recurring intervals and customized to run the job multiple times in a day or months.
- Audit Logs are captured in the logging subsystem.

Audit

- The auditing is enabled subsystem-wise (ADC+ and CERT+) based on internal business logic.
- Notification logs and Audit logs are captured for each internal business logic.

For the full list and details of scheduled jobs supported in CERT+, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling/Disabling a Job

1. Go to (**Menu**) > **CERT+** > **Administration** > **Job Scheduler**.
2. Under **Task Name**, for the **required job** job, click the **Enabled**/**Disabled** toggle key.
   The key label shows the current job status.

Modifying the Configuration of a Job

1. Under **Task Name**, select the required job.
   A dialog box with the configuration for the selected job is displayed.
2. Update the job configuration as required and click **Update**.

Field descriptions for the job configuration

Frequency Type	Description
Description	Enter details related to the job. **Note:** Character limit: **2000 characters**
Time Zone	From the dropdown list, select the time zone in which the job will be triggered.
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Minutes**
***Starts On**	Click **(Calendar** widget) to select a date to start triggering the job.
***Repeat**	(Optional) For **Occurrence Type** = **Daily**, from the dropdown list, select the number of **Times** a job should be triggered in the course of a day. (Mandatory) For **Occurrence Type** = **Minutes**, from the dropdown list, select the interval, in **Minutes**, after which the job should be triggered.
***Repeat On**	For **Occurrence Type** = **Weekly**, select the checkbox corresponding to the day of the week on which the job should be triggered.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Summary	Displays a summary of the selections made for the job schedule.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 4: CERT+ API Guide

This guide provides information on the APIs to use for various CLM actions.

API Reference

To try the AppViewX exposed APIs on Swagger, follow these steps:

1. From the top right corner of your screen, click {...} **(API Reference)** icon.

   Note: The **API Reference** icon is displayed for the Admin user and users with ACF permission enabled for API Reference.

   You will be redirected to **AppViewX API Reference** page.

2. Click the required API to **Try it out**.

Enable ACF Permission for API Reference

To enable the ACF permission for non-admin roles to access the API reference, follow these steps:

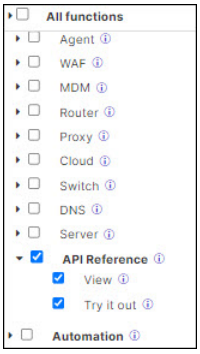
1. Go to **Platform** module **IDENTITY** > **Role**.

   You will be redirected to **Role** page.

2. Click on the role name to enable the ACF permission.

   You will be redirected to the **Modify :: [RoleName]** page, with the **Information** tab open by default.

3. Switch to the **Authorized Functions** tab and expand the **Platform** by clicking **(Expand)** icon.
4. To assign **API Reference**, select the checkbox beside **API Reference**.



5. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Best Practices for Working with the AppViewX API

- **Use appropriate HTTP methods.**

  Ensure that the correct HTTP method is used for each operation (e.g., GET for retrieval, POST for creation).

- **Handle errors gracefully.**

  Implement proper error handling in your application to manage API responses.

- **Use secure storage.**

  Store access tokens securely and avoid hardcoding them in your application code.

- **Implement pagination.**

  For endpoints that return large datasets, implement pagination using limit and offset parameters.

- Understanding the AppViewX CERT+ API
- Authentication using a User Account
- Authentication using a Service Account
- CLM API
- ADC+ API (for CERT+)
- MultiCloud API
- Automation Workflows API
- After you are done

Understanding the AppViewX CERT+ API

The AppViewX CERT+ API provides a set of RESTful endpoints for managing certificates across your infrastructure. This section covers how to make requests, handle responses, and understand the structure of the API.

RESTful HTTPS Requests

The CERT+ API uses RESTful principles, leveraging standard HTTP methods to interact with resources. All requests must be made over HTTPS to ensure security.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Type	Description
GET	GET requests, retrieve resource representation/information only and not to modify it.
POST	POST APIs create new subordinate resources. For example, a file is subordinate to a directory containing it or a row is subordinate to a database table. In terms of REST, POST methods are used to create a new resource into the collection of resources.
PUT	PUT APIs are used to update existing resources (if a resource does not exist then API may decide whether to create a new resource or not).
DELETE	DELETE APIs are used to delete resources (identified by the Request-URI).

Requests

All API endpoints are accessed via the following base URL. The base URL is built in the same way by the following structure:

```
http://<IP/HostName/TenantName>:<GWPORT>/avxapi/<Endpoint>?<gwsource>
```

Explanation

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Request Structure

All endpoints accept a request structure that should consist of JSON formatted data. To ensure the request is accepted, set the header **Content-Type: application/json**.

The following example shows a request to add a resource:

```
{
"payload": {
"name": "resource_1",
"description": "This is a sample resource."
}
}
```

Response Structure

The Content-Type of the response is typically determined by the Content-Type header, and for most endpoints, it will be application/json. All requests that reach the server, regardless of the response code, will retrieve a response body. A successful request will contain a body with the requested information, for example:

```
https://appviewxapi.com/avxapi/resource?gwkey=f000ca01&gwsource=external
```

Returns the following JSON structure that a resource is added:

```
{
"response": "Resource added successfully",
"message": "Resource added successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Description of Server Responses

HTTP Code	Response Message
200 OK	The request was successful (some API calls may return 201 or 202 instead).
400 Bad Request	The request is not understood or required parameters are missing.
401 Unauthorized	Authentication failed or the user doesn't have permissions for the requested operation.
409 Forbidden	Access denied.
404 Not Found	Resource not found.
429 Too many requests	The number of requests to the service has crossed the threshold.
503 Service unavailable	The client cannot communicate with the service.
504 Gateway timeout	The given request has exceeded the expected time.

URI Scheme

- **Host :** {url}
- **BasePath :** /avxapi
- **Schemes :** HTTPS
- **URL :** https://{url}/avxapi

Types of Accounts in AppViewX

There are two types of accounts in AppViewX:

- **User Accounts**: These are used by actual users.
- **Service Accounts**: These are used by system services such as web servers, automation tools, and so on.

AppViewX recommends using a Service Account for accessing APIs from automation tools. Service Accounts are supported with oAuth standard for a more secure and standard way of accessing APIs.

Note: AppViewX supports both User Account and Service Account for accessing APIs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Authentication using a User Account

For accessing APIs using a User account:

- **User Account**

  A **user account** represents an individual person interacting with the application or the system. User accounts are used for accessing the system on behalf of a user.

  For accessing APIs with a user account, you need to get the session ID by providing a username and password in the Login API. This session ID can then be used for accessing other APIs.

  Note: You can also use the username and password in all API calls instead of the sessionId. However, this is not recommended.

- Retrieve session ID using login API
- Using Session ID for further API calls

Retrieve session ID using login API

This API used to retrieve the session ID using the login API for secure authentication and access to system resources.

Before you begin

- Make sure you have valid login credentials (Username and Password) for accessing the system.
- You cannot use OAuth credentials (Client ID and Client Secret) for login.
- To access the APIs using the service token, use the API with the Service Account.

Request Structure

Endpoint	`/login`
Type	`POST`
Sample URL	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/login?&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request timeout period	15 minutes

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

	Description
username	(Mandatory) Use login name of the user.
Header	**Type:** String
	Example: "admin"
password	(Mandatory) Password for the username.
Header	**Type:** String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

	Description
	Example: "AppViewX@123"
otp *Header*	(Mandatory only if MFA is enabled) If MFA is enabled, enter the OTP received on your registered email ID in the header. Multifactor authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a resource If MFA is enabled, and you try to login with only the username and password, you will get the following error upon execution of the API: **MFA is enabled. We have sent an OTP to your email ID: aaa********r@appviewx.com**. In this case, ensure that the OTP is included in the header and try logging in again. **Type:** String **Example:** "OTP : **609700**"
Content-Type *Header*	(Mandatory) The parameter should be set to `application/json` to specify the nature of the data in the payload. **Type:** String **Example:** "application/json"
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** String

Response Structure

- **Status Code:** 200 Ok
- **Message:** Login Successful
- **Headers:**
  - **Content-Type:** application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters

Name	Description
response	The response contains the attributes needed to retrieve the session ID.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Name	Description
status	Indicates the overall status of the response. The values can be: • SUCCESS • FAILURE
appStatusCode	An application-specific status code, if applicable.
statusDescription	Description of the status, if available.
sessionId	Unique identifier for the session.
lockDownPeriod	Number of login attempts remaining.
termsAccepted	
passwordExpiryMsg	
emailId	

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Login successful
400 Bad request	ACCT_AUTH_001	Username or password cannot be null or empty.
401 Unauthorized	ACC_AUTH_022	Login failed. Invalid credentials.
401 Unauthorized	ACC_AUTH_006	Login failed. Invalid credentials.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Use Case

Log in to the application with a username and password.

Sample Request URL

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/login?&gwsource=external
```

Request Payload

```
{}
```

Sample Response


```
{
    "response": {
        "status": "SUCCESS",
        "appStatusCode": null,
        "statusDescription": null,
        "sessionId": "avx~~c73a4f56-f4ab-4cdf-aadf-6d90bf406077",
        "authCode": null,
        "lockDownPeriod": 15,
        "emailId": null,
        "termsAccepted": true,
        "passwordExpiryMsg": ""
    },
    "message": "Login successful.",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


What's next?

After the sessionID is retrieved using the login API, you can now use the session ID for API calls.

Using Session ID for further API calls

The sessionID retrieved using the login API can be used in the header for making further API calls.

In this section, as an example, we are using the session ID with the API call for reissuing a certificate in the async mode.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting must be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting is working fine.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
userName *Header*	(Mandatory only if **sessionID** is not provided) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload	Contains all the parameters to be sent in the request body for the put request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Body	**Type**: Payload

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the reissue. **Type**: String **Possible values**: Reissue
reason	(Mandatory) Reason for reissue request. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response attributes for the reissue request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Work order request Id. **Type**: String
message response	Success message - Reissue action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open workOrder for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the reissue action. • There is no workOrder in progress for the specified certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		• Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload


```
{
"commonName":"testcert8g.appviewx.plus",
 "serialNumber":"08:BD:54:35:FD:81:AC:A4:45:2B:FC:9F:77:56:FE:2C",
 "action":"Reissue",
 "reason":"Superseded"
 }
```


Response


```
{
"response": {
"resourceId": "5f51f7312fa95059a12b0aee",
"message": "Reissue action triggered successfully.",
"requestId": "238"
},
"message": "Reissue action has been triggered successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Authentication using a Service Account

For accessing APIs using a Service account:

- **Service Account**

  A **service account** represents a non-human entity such as an application or a service. It is used for automated processes or system-to-system interactions without human intervention.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For accessing APIs with a service account, you need to get the Access Token by providing Client ID and Client Secret in get-service-token API. This Access Token can then be used for accessing other APIs.

Note: Access Token Validity is 30 minutes by default and it can be configured in **Settings** > **Authentication** > **oAuth Settings**.

- Retrieve Access Token using get-service-token API
- Using Access Token in the header for further API calls

Retrieve Access Token using get-service-token API

The API provides a streamlined process for retrieving service tokens related to account management tasks.

Before you begin

- Make sure you have valid login credentials for accessing the system.

Request Structure

Endpoint:	/acctmgmt-get-service-token
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-get-service-token?gwsource=external To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json
Authentication:	Yes
Request timeout period	15 minutes

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

	Description
Authorization *Header*	(Mandatory) Please form a string in this format <Client ID>:<Client Secret> and do base64 encoding. Then prepend a key 'Basic' before the encoded value. Final value should be "Basic <EncodedValue>". **Type:** *String* **Example:** "admin"
Content-Type *Header*	(Mandatory) The parameter should be set to `application/json` to specify the nature of the data in the payload. **Type:** *String* **Example:** "application/json"

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

	Description
grant_type *Payload*	(Mandatory) Payload Type should be "Form". The value of the param should be "Client_Credentials". **Type:** *Text*

Response Structure

- **Status Code:** 200 Ok
- **Message:** Successful
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	The response contains the attributes needed to retrieve the access token.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Successful
400 Bad request	ACCT_SA_003	Service account is invalid/not found::[Service account not found in the database]
400 Bad request	OAUTH_CLNT_015	Client Password is incorrect::[Invalid Client credential]
400 Bad request	ACCT_SA_001	Invalid Request::[Invalid client Id or secret]
500 Internal Server Error	avx-common-011	Error while processing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Use Case

Retrieve Access Token.

Request URL

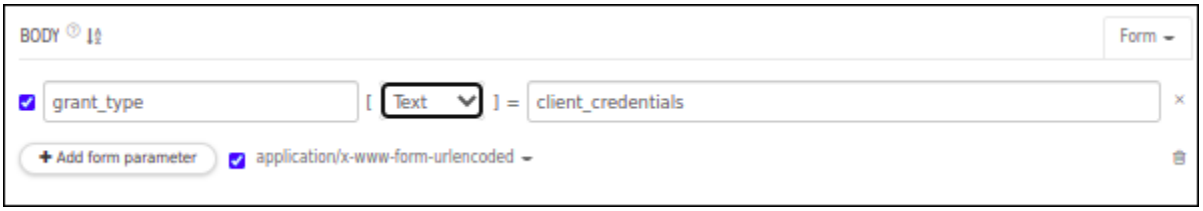
```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/acctmgmt-get-service-token?gwsource=external
```

Content-Type: application/x-www-form-urlencoded

Authorization: Basic

```
NTIxYzNhZDItZWE0ZS00NDdiLWE1MWItOTYyMWJiN2VhMTI2OjU1QVUjTk84JSpaaGd2TmZhWVVtdHZYMGRrRWhvZGJpCg==
```

Request Payload



Sample Response

```
{
"response":
 "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBj
 NGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncmFudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqIDI7
 GYf4cWx6VwbjGD_0",
"message": null,
"appStatusCode": null,
"tags":{},
"headers": null
}
```

Using Access Token in the header for further API calls

The access token retrieved using the get-service-token API can be used in the header for making further API calls.

In this section, as an example, we are using the access token with the API call for reissuing a certificate in the async mode.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

- Access Token is obtained from the get-service-token API.
- Ensure that the Access Token is valid and has not expired.

Request Structure

Endpoint:	`/certificate/create`
Type:	`POST`
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external` To understand the elements of the sample URL, click here.
Headers:	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
Token *Header*	(Mandatory) Use token retrieved from login API. **Type:** *String* **Example:** eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJwbGF0Zm9ybSIsImF1ZCI6ImF2eCIsImNsaWVudElkIjoiOTcwNzRlNDEtOGFmOS00NTZkLTlhNjQtZjBjNGJiOTA4MDQ4IiwiaXNzIjoiYXZ4IiwiZXhwIjoxNjUwMzY5MzY3LCJncmFudCB0eXBlIjoiY2xpZW50X2NyZWRlbnRpYWxzIn0.HZnkuUEjXIeqJWqpqiNWFHqIDI7GYf4cWx 6VwbjGD_0
gwsource *Query*	(Mandatory) Source from which the request is triggered. The values can be: • web • external **Type:** *String*
Payload *String*	(Mandatory) Input data for request body in application/json format. For payload details, see Payload section.

Payload

Name	Description
name *String*	(Mandatory) Name of the resource to create. Name cannot be duplicated. **Example:** "resource_1"
description *String*	(Optional) Description of the resource. **Example:** "This is a sample resource."

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

- **Status Code:** 201 Created
- **Message:** Resource added successfully
- **Headers:**
  - **Content-Type:** application/json

Response Parameters

Name	Description
response	Contains the response attributes for resource added successfully.
message	Success message or failure description in case of error.
appStatusCode	Application specific status code for the response. Will be non-null for failure response.
tags	More info in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
201 Created	null	Resource added successfully
409 Conflict	RBAC_RE_005	Resource with the given name already exists
400 Bad Request	VALIDATION_ERROR_0004	'name' should have at least '2' characters, Mandatory Field 'name' is missing or empty
400 Bad Request	VALIDATION_ERROR_0004	Invalid "name".
401 Unauthorized	AVX_GW_012	Unauthorized access, reason - Invalid Token
407 Proxy Authentication Required	AVX_GW_011	Session validation failed, reason - Session information is missing.

Sample Request/Response

Use Case

Add a resource using API with Access Token.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource?gwsource=external
```

Request Payload

```
{
 "payload": {
 "name": "resource_1",
 "description": "This is a sample resource."
 }
 }
```

Sample Response

```
{
 "response": "Resource added successfully",
 "message": "Resource added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
 }
```

CLM API

- Create a Certificate in Async mode
- Create a Certificate in Sync mode
- Renew a Certificate in Async mode
- Renew a Certificate in Sync mode
- Revoke a Certificate in Async mode
- Revoke a Certificate in Sync mode
- Reissue a Certificate in Async mode
- Reissue a Certificate in Sync mode
- Regenerate a Certificate in Async mode
- Regenerate a Certificate in Sync mode
- Suspend a Certificate
- Reinstate a Certificate
- Search/Get Certificate Inventory

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Add Certificate Attributes
- Add Multiple Certificate Attributes
- Update Certificate Attributes
- Get Certificate Attributes
- Delete Certificate Attributes
- Delete Multiple Certificate Attributes
- Bulk Add/Update Certificate Attributes
- Fetch List of Server Devices
- Download a Certificate
- Download a Certificate by Format
- Download Private Key of a Certificate
- Common Response Objects
- Push and Bind Certificate to a Firewall Profile
- Rollback Certificate to Firewall Profile
- Get Available Server Profiles
- Push and Bind Certificate to a Server Profile
- Rollback Certificate to Server Profile
- Delete Certificate using UUID
- Discover Certificates from Firewall
- Discover Certificates from Server
- Discover Certificates from CT Log
- Discover Certificates from Network
- Network Discovery Configuration
- Fetch Single Certificate Discovery
- Fetch Certificate Discovery Results by Discovery Name
- Fetch Devices Discovered During a Network Scan
- Fetch Cipher–TLS Version Mapping from Discovery Execution
- Delete Certificate Discovery
- Upload Multiple Certificates to the Inventory
- Upload Server Certificate to the Inventory
- View a Certificate Group
- Create a Certificate Group
- Update a Certificate Group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Delete a Certificate Group
- Assigning ACL Permissions for Resources
- Trigger Profile Sync for Devices
- List Certificates with Application Connector Details
- List Certificate Groups
- Use Insights to Create a Centralized CERT+ Dashboard
- Assign Certificates to a Group
- Unassign Certificates from a Group
- Archive Certificates
- Recover Archived Certificates

Create a Certificate in Async mode

The API initiates the creation of a new certificate in async mode. This mode requests certificate generation and provides a request ID in the response. The request payload varies depending on the Certificate Authority (CA) used for enrollment. After successfully triggering the create certificate API, the response includes the resourceId, which can be used to activate the search API and retrieve the created certificate. Please refer to the After you are done section for instructions on approving and implementing the request.

Before you begin

Ensure the following before attempting to enroll a certificate from a particular CA through AppViewX:

- The CA must configured in AppViewX from the Certificate Authority page.
- The user should have the ACF permission to submit certificates within the specified certificate's category.
- The group associated with the certificate must have RW permission.
- Connectivity to the CA via the chosen setting should be working correctly.
- A certificate group should be created and associated with the policy. If not, the certificate will be created under the Default group.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/create
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/create?gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Payload	Contains all the parameters to be sent in the request body for the post request.
Body	**Type**: Payload

Payload

Payload

Name	Description
csrGenerationSource	(Optional) Specifies where the CSR is to be generated. **Type**: **Possible values:**: appviewx, uploadCSR, ENDPOINT, hsm. **Default value**: appviewx
caConnectorInfo	(Mandatory) Details related to the certificate authority (CA) and the CSR parameters. **Type**: Any of the following data: • Amazon caConnectorInfo • AppViewX caConnectorInfo • DigiCert caConnectorInfo • EJBCA caConnectorInfo • Entrust caConnectorInfo • EntrustMPKI caConnectorInfo • GlobalSign caConnectorInfo • GoDaddy caConnectorInfo • Google caConnectorInfo • InCommon caConnectorInfo • LetsEncrypt caConnectorInfo • Microsoft Enterprise caConnectorInfo • Microsoft Standalone caConnectorInfo • OpenTrust caConnectorInfo • Sectigo caConnectorInfo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	• Symantec caConnectorInfo • Trustwave caConnectorInfo
certificateGroup	Specifies the group (category) to which the newly created certificate should be assigned. **Type**: certificateGroup **Constraint**: Default certificate Group is "**Default**".
deviceDetails	(Optional) Information about the device or endpoint where the Certificate Signing Request (CSR) will be generated. **Type**: deviceDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **Endpoint**.
certificateHSMDetails	(Optional) Information about the Hardware Security Module (HSM) device. **Type**: certificateHSMDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **HSM**.
uploadCsrDetails	(Optional) Information about the CSR. **Type**: uploadCsrDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **uploadCSR**.
certificateFormat	(Optional) Certificate download format details. **Type**: certificateFormat

certificateGroup

Name	Mandatory
name	(Optional) Specifies the group under which the created certificate needs to be tagged. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateGroup (continued)

Name	Mandatory
	Constraint: The certificate group must be present in AppViewX.

deviceDetails

Name	Mandatory
category	(Mandatory) Specifies the device category **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor	(Mandatory) Name of the vendor for the chosen device. For example, **Apache** is a vendor for **Server** category. **Type**: String
deviceName	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
csrFileName	(Mandatory) Name of the CSR file that is generated in the device. **Type**: String
keyFileName	(Mandatory) Name of the key file that is generated in the device. **Type**: String
attributes	(Optional) Additional attributes for the chosen device as mentioned the sub-attributes - csrLocation, tenant, and partition. **Type**:
csrLocation attributes	(Optional) The location within the device where the CSR is generated. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Server** and the **deviceDetails.vendor** is **Tomcat**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

deviceDetails (continued)

Name	Mandatory
tenant attributes	(Optional) Name of the partition within the AVI device. **Type**: String
partition attributes	(Optional) Name of the partition within the device. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Friewall** and the **deviceDetails.vendor** is **Fortinet**.

certificateHSMDetails

Name	Mandatory
type	(Mandatory) Type of the HSM device. **Type**: String **Possible values**: ADC and HSM.
keyReference	(Mandatory) Reference name for the key that is mapped by the HSM device. **Type**: String
hsmSettings	(Mandatory) Configuration details for the HSM device. Contains the sub-parameters vendorType and vendorSpecificSettings **Type**: List <String>
vendorTypehsmSettings	(Mandatory) Category of the vendor. **Type**: String **Possible values**: Safenet, Thales, and Fortanix.
vendorSpecificSettingshsmSettings	(Mandatory) Settings related to HSM vendor. Contains the sub-parameter moduleId

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateHSMDetails (continued)

Name	Mandatory
	Type: String
moduleId `hsmSettings. vendorSpecificSettings`	(Optional) The module id. **Type**: String **Constraints**: Applicable if **hsmSettings.vendorType** is **Thales**.
vendor	(Mandatory) The name of the vendor for the chosen device e.g., F5. **Type**: String
deviceName	(Mandatory) The name of the device as per AppViewX Device Inventory. **Type**: String

uploadCsrDetails

Name	Mandatory
category	(Mandatory) Certificate category **Type**: String **Possible values**: Server, Client, and Code Signing
csrContent	(Mandatory) The CSR content for certificate enrollment request **Type**: String

certificateFormat

Name	Mandatory
format	(Mandatory) Certificate download format. Refer to the Possible values for Certificate Download Format table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateFormat (continued)

Name	Mandatory
	Type: String
password	(Optional) The field is mandatory for some parameters (refer to the table below). **Type**: String

Possible Values for Download Format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.pk12	PK12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
resourceId response	Identifier of the certificate record that has been created (the resourceId in the above request can be found using the search API using commonName, serial No. or other search parameters). **Type**: String
requestId response	Open work order request ID. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate submission triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_CSR_GEN_SOURCE	Invalid csr generation source specified. **Remediation**: Ensure that a valid value is provided for the csrGenerationSource field in the request.
417 Expectation failed	READ_GROUP	Group is given with read permission, so cannot perform any operation. **Remediation**: Ensure that the field csrGenerationSource field has read write permission.
404 Expectation failed	GROUP_NOT_FOUND	Invalid group name specified. **Remediation**: Ensure that a valid value is provided for the certificateGroup section in the request.
404 Not Found	CERT-CA-0001	CA settings are not available. **Remediation**: Ensure that a valid value is provided for the caSettingName section in the request.

What's next?

Add Certificate Attributes

Download a Certificate

Download a Certificate by Format

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.
- CA Specific Information
- Common Payload Objects

CA Specific Information

Payload structure, sample request/response and the possible response codes for all the supported CAs are as follows:

- Amazon
- AppViewX
- DigiCert
- EJBCA
- Entrust
- Entrust MPKI
- GlobalSign

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- GoDaddy
- Google
- InCommon
- Let’s Encrypt
- Microsoft Enterprise
- Microsoft Standalone
- OpenTrust
- Sectigo
- Symantec
- Trustwave

Amazon

Amazon Request Objects

Amazon caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Amazon**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Amazon caConnectorInfo (continued)

Name	Description
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Amazon CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Amazon genericFields
name	(Optional) Name for the CA connector. **Type**: String

Amazon CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Amazon CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Amazon CSR Parameters (continued)

Name	Description
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Amazon genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload

```
{
 "csrGenerationSource": "appviewx",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"caConnectorInfo": {
"certificateAuthority": "Amazon",
"isAutoRenewal": false,
"autoRegenerateEnabled": false,
"caSettingName": "Amazon",
"certificateType": "",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
"Server",
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testamazon.appviewx.com"
]
}
},
"genericFields": {
"device_name_Amazon": "",
"vs_ip_Amazon": ""
},
"vendorSpecificDetails": {
"orderId": ""
}
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "149"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


AppViewX

AppViewX Request Objects

AppViewX caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **AppViewX**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX caConnectorInfo (continued)

Name	Description
	If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateProfileName	(Optional) Determines the category of certificate that is being requested. **Type**: String **Constraint**: Possible values - Server, Client, and Code Signing. The default value is Server.
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: AppViewX CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: AppViewX genericFields
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX caConnectorInfo (continued)

Name	Description
	Type: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

AppViewX CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload


```
{
 "csrGenerationSource": "appviewx",
 "caConnectorInfo": {
 "certificateAuthority": "AppViewX",
 "isAutoRenewal": false,
 "autoRegenerateEnabled": true,
 "regenerateBeforeInDays": "30",
 "caSettingName": "AppViewX CA",
 "certificateProfileName":"Server",
 "description": "",
 "csrParameters": {
 "commonName": "testcert.testdomain.com",
 "organization": "AppViewX",
 "organizationUnit": "PE",
 "locality": "Plano",
 "state": "Texas",
 "country": "US",
 "mailAddress": "test@test.com",
 "hashFunction": "SHA256",
 "keyType": "RSA",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"bitLength": "2048",
"certificateCategories": ["Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": ["*.testcert4d.appviewx.com, testcert4b1.avx.com"],
"iPAddresses": ["xxx.xxx.xxx.xxx"]
}
},
"genericFields": {
"device_name_AppViewX": "test_device",
"vs_ip_AppViewX": "192.168.142.162"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4842fd70040d33314f0748",
"requestId": "135"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

DigiCert

DigiCert Request Objects

DigiCert caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Digicert**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

DigiCert caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
divisionId	(Mandatory) Digicert division id. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Digicert CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Digicert genericFields
vendorSpecificDetails	(Optional) Data specific to the Digicert vendor. **Type**: Digicert vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

DigiCert caConnectorInfo (continued)

Name	Description
	Type: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

Digicert CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Digicert CSR Parameters (continued)

Name	Description
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Digicert CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Digicert genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Digicert vendorSpecificDetails

Name	Description
caCertId	(Optional) Certificate id for the chosen certificate authority. **Type**: String **Constraint**: It is **mandatory** for DigiCert private product types e.g. "Private SSL Plus."
serverType	(Optional) The server category to which the certificate is requested, such as AOL. **Type**: String

Sample Request/Response

Request Payload

```
{
 "csrGenerationSource": "ENDPOINT",
"deviceDetails":
{
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"vendor": "Apache",
"category": "Server",
 "deviceName": "Apache server",
"csrFileName": "test",
 "keyFileName": "test",
"attributes":
{
 "csrLocation": ""
 }
 },
"caConnectorInfo":
{
 "certificateAuthority": "DigiCert",
"isAutoRenewal": false,
 "autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "DigiCert",
"divisionId": "80312",
"certificateType": "Private SSL Plus",
 "description": "", "csrParameters":
{
 "commonName": "testcert8g.appviewx.plus",
"organization": "AppViewX Inc.",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
 "certificateCategories": ["Server"],
"ellipticCurve": "", "enhancedSANTypes":
{
"dNSNames": []
 }
},
 "genericFields":
{
 "device_name_DigiCert": "test_device",
 "vs_ip_DigiCert": "xxx.xxx.xxx.xxx"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
},
"vendorSpecificDetails":
{
"caCertId": "741B2D2F05C7F6543EFB",
"serverType": "Apache" },
"validityUnitValue": "1",
"validityInDays": 365,
"validityUnit": "years"
},
"certificateGroup":
{
"name": "Default"

}
}
```


Response


```
{
"response":
{
"resourceId": "5f4faf3e70040d33314f1142",
"requestId": "173"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


EJBCA

EJBCA Request Objects

EJBCA caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EJBCA caConnectorInfo (continued)

Name	Description
	Type: String **Constraint**: The value should be **Ejbca**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EJBCA caConnectorInfo (continued)

Name	Description
	Constraint: *Prerequisite* - End entity profiles should have been fetched and updated in the specified CA setting.
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Ejbca CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Ejbca genericFields
vendorSpecificDetails	(Optional) Data specific to the Ejbca vendor. **Type**: Ejbca vendorSpecificDetails
customAttributes	(Optional) Custom fields configured for EJBCA.
postalCode `customAttributes`	(Optional) This field is given as an example, there could be any number of fields as specified in the policy. **Type**: String
name	(Optional) Name for the CA connector. **Type**: String

EJBCA CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EJBCA CSR Parameters (continued)

Name	Description
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EJBCA CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EJBCA CSR Parameters (continued)

Name	Description
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, rfc822Names, iPAddresses and uniformResourceIdentifiers.
dNSNames	(Optional) List of subject alternative names for the certificate.
`enhancedSANTypes`	**Type**: Array of String
rfc822Names	(Optional) Email addresses to be considered as Subject Alternative Names.
`enhancedSANTypes`	**Type**: Array of String
iPAddresses	(Optional) List of IP address to be considered as subject alternative names.
`enhancedSANTypes`	**Type**: Array of String
uniformResourceIdentifiers	(Optional) URIs to be considered as Subject Alternative Names.
`enhancedSANTypes`	**Type**: Array of String

EJBCA genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EJBCA vendorSpecificDetails

Name	Description
userName	(Optional) The username configured at the CA's end. **Type**: String
endEntityProfileName	(Mandatory) The name of the end-entity profile configured at the CA's end. **Type**: String
issuerCommonName	(Mandatory) The common name of the issuer configured at the CA's end. **Type**: String
certificateProfileName	(Mandatory) The name of the certificate profile selected from the available options for the chosen "endEntityProfile." **Type**: String

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Ejbca",
"isAutoRenewal": false,
"autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "ejbca",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"locality": "Plano",
"state": "Texas",
"country": "US",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": ["testcert5.avx.com"],
"rfc822Names": ["test@testcert5.avx.com"],
"iPAddresses": ["xxx.xxx.xxx.xxx"],
"uniformResourceIdentifiers": ["http://testcert5.avx.com"]
}
},
"genericFields": {
"device_name_Ejbca": "test_device",
"vs_ip_Ejbca": "192.168.142.162"
},
"vendorSpecificDetails": {
"userName": "",
"endEntityProfileName": "APPVIEWX PROFILE",
"issuerCommonName": "Ejbca New Intermediate CA",
"certificateProfileName": "SERVER PROFILE"
},
"customAttributes": {}
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "147"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

Entrust

Entrust Request Objects

Entrust caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Entrust**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust caConnectorInfo (continued)

Name	Description
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
divisionId	(Mandatory) Entrust division id. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Entrust CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Entrust genericFields
vendorSpecificDetails	(Optional) Data specific to the Entrust vendor. **Type**: Entrust vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust caConnectorInfo (continued)

Name	Description
	Constraint: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
customAttributes	(Optional) Custom fields configured for Entrust, such as email1.
email1 `customAttributes`	(Optional) The field "email1" is given as an example. Multiple custom attributes could be configured. **Type**: String
name	(Optional) Name for the CA connector. **Type**: String

Entrust CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust CSR Parameters (continued)

Name	Description
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, and uniformResourceIdentifiers.
dNSNames	(Optional) List of subject alternative names for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust CSR Parameters (continued)

Name	Description
`enhancedSANTypes`	**Type**: Array of String
iPAddresses	(Optional) List of IP address to be considered as subject alternative names.
`enhancedSANTypes`	**Type**: Array of String
uniformResourceIdentifiers	(Optional) List of URIs to be considered as subject alternative names.
`enhancedSANTypes`	**Type**: Array of String

Entrust genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Entrust vendorSpecificDetails

Name	Description
additionalEmails	(Optional) Additional emailID to be associated with the request. **Type**: String **Constraint**: It should be a valid email address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Entrust",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "Entrust",
"certificateType": "Standard",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Server"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [],
"iPAddresses": [],
"uniformResourceIdentifiers": []
}
},
"genericFields": {
"device_name_Entrust": "test_device",
"vs_ip_Entrust": "xxx.xxx.xxx.xxx"
},
"vendorSpecificDetails": {
"additionalEmails": "test1@test.com"
},
"customAttributes": {
"email1": "test@test.com",
"text2": "ID12345",
"dropdown1": "Server Cert",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"number1": "1",
"date1": 1598985000000
},
"validityInDays": 90
},
"certificateGroup": {
"name": "Default"
}
```


Response


```
{
"response": {
"resourceId": "5f4fcb1770040d33314f11f0",
"requestId": "184"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Entrust MPKI

Entrust MPKI Request Objects

Entrust MPKI caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Entrust MPKI**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust MPKI caConnectorInfo (continued)

Name	Description
	Constraint: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust MPKI caConnectorInfo (continued)

Name	Description
	Type: Entrust MPKI CSR Parameters
vendorSpecificDetails	(Optional) Data specific to the Sectigo vendor. **Type**: Entrust MPKI vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

Entrust MPKI csrParameters

Name	Mandatory	Description	Field Type	Constraints
commonName	Yes	Fully qualified domain name (FQDN) of the server for which certificate is requested.	String	Must be compliant with the common name specified in the policy, if

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust MPKI csrParameters (continued)

Name	Mandatory	Description	Field Type	Constraints
				the policy is set as ‘Strict’.
organization	No	Legal name of the organization.	String	Default value - Value configured in the policy.
organizationUnit	No	Division or department of the organization handling the certificate.	String	Default value - Value configured in the policy.
locality	No	City where the organization is located. This shouldn't be abbreviated.	String	Default value - Value configured in the policy.
state	No	State or region where the organization is located.This shouldn't be abbreviated.	String	Default value - Value configured in the policy.
country	No	The two-letter code for the country where your organization is located.	String	Default value - Value configured in the policy.
mailAddress	No	Email address of the organization.	String	Default value - Value configured in the policy.
hashFunction	No	Hash function to be used in the Certificate. For example, SHA160.	String	Default value - the first value will be chosen from the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust MPKI csrParameters (continued)

Name	Mandatory	Description	Field Type	Constraints
		Should be chosen from the possible values configured in the Certificate Policy.		
keyType	No	Algorithm to be used for Key generation. For example, RSA, DSA, EC. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
bitLength	No	Bit length for the key is dependent on the key type chosen. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
certificateCategories	Yes	Purpose for which the generated certificate will be used.	Array	Possible values - Server, Client, Code Signing, Email
ellipticCurve	No	If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bitlength selected. Should be chosen from the possible values configured in the Certificate Policy.	String	Default value - the first value will be chosen from the policy.
enhancedSANTypes	No	Subject alternative names for the certificate.	Entrust MPKI enhancedSANTypes	Value provided must be

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Entrust MPKI csrParameters (continued)

Name	Mandatory	Description	Field Type	Constraints
				compliant with the Certificate Policy, if the policy is configured as Strict.

Entrust MPKI vendorSpecificDetails

Name	Mandatory	Description	Field Type	Constraints
caName	Yes	Name of the CA.	String	Should be a valid CA name configured in CA Settings.
certProfile	Yes	Certificate Profile name associated with the given caName.	String	Should be a valid Certificate Profile name configured in CA Settings.

Entrust MPKI enhancedSANTypes

Name	Mandatory	Description	Field Type	Constraints
dNSNames	No	List of Subject Alternative names for the Certificate.	Array of String	NA
iPAddresses	No	IP addresses to be considered as Subject Alternative Names.	Array of String	Must be valid ip addresses.
uniformResourceIdentifiers	No	URIs to be considered as Subject Alternative Names.	Array of String	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GlobalSign

GlobalSign Request Objects

GlobalSign caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **GlobalSign**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GlobalSign caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String **Constraint**: Possible values - Alpha SSL, Domain SSL, Organization SSL, and Extended SSL.
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: GlobalSign CSR Parameters
vendorSpecificDetails	(Optional) Data specific to the GlobalSign vendor. **Type**: GlobalSign vendorSpecificDetails **Constraint**: Mandatory for the following "cerificateTypes" - Alpha SSL, Domain SSL, and Extended SSL.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GlobalSign CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GlobalSign CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GlobalSign CSR Parameters (continued)

Name	Description
	Recommendation: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String

GlobalSign vendorSpecificDetails

Name	Description
domainAdminMailId	(Mandatory) The local-part of the email address for the administrator or group responsible for issuing and approving certificate requests. For instance, in hostmaster@test.com, "hostmaster" is the local-part. **Type**: String
incorporatingAgencyRegistrationNumber	(Optional) The registration number of the company. **Type**: String **Constraint**: It **mandatory** if the "certificateType" is **extendedSSL**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GlobalSign vendorSpecificDetails (continued)

Name	Description
designation	(Optional) The designation of the authorized signer. **Type**: String **Constraint**: It **mandatory** if the "certificateType" is **extendedSSL**.
businessCategory	(Optional) The category code for the business type. **Type**: String **Constraint**: It **mandatory** if the "certificateType" is **extendedSSL**.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "GlobalSign",
"autoRegenerateEnabled": false,
"caSettingName": "Globalsign",
"certificateType": "Alpha SSL",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"streetAddress": "Park Street",
"locality": "Plano",
"state": "Texas",
"country": "US",
"postalCode": "73301",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"bitLength": "2048",
"certificateCategories": ["Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"vendorSpecificDetails": {
"domainAdminMailId": "hostmaster",
"incorporatingAgencyRegistrationNumber": "",
"designation": "",
"businessCategory": "PO",
"orderId": ""
},
"validityInDays": 183
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e876e70040d33314f0f0b",
"requestId": "149"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GoDaddy

GoDaddy Request Objects

GoDaddy caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **GoDaddy**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GoDaddy caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: GoDaddy CSR Parameters
vendorSpecificDetails	(Optional) Data specific to the GoDaddy vendor. **Type**: GoDaddy vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String

GoDaddy CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GoDaddy CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GoDaddy CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GoDaddy vendorSpecificDetails

Name	Description
firstName	(Optional) User's first name as configured in GoDaddy. **Type**: String
lastName	(Optional) User's last name as configured in GoDaddy. **Type**: String
emailAddress	(Optional) Email address of the user to be configured at the CA. **Type**: String **Constraint**: It should be a valid email address.
phone	(Optional) Phone number of the user. **Type**: String
apiKey	(Mandatory) API key to be used for GoDaddy CA communication. **Type**: String
apiSecret	(Mandatory) API secret to be used for GoDaddy CA communication. **Type**: String
customerNumber	(Mandatory) Customer number obtained from the user's GoDaddy portal. **Type**: String
url	(Mandatory) Base URL to be used for GoDaddy CA communication. **Type**: String

Sample Request/Response

Request Payload

```
{
"certificateGroup": {
"name": "Default"
},
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"caConnectorInfo": {
"name": "GoDaddy Deluxe UCC SSL SAN UCC OV SSL connector",
"description": "",
"certificateUuid": "",
"certificateAuthority": "GoDaddy",
"certificateType": "Deluxe UCC SSL - SAN (UCC_OV_SSL)",
"csrParameters": {
"commonName": "testgodaddy",
"organization": "",
"locality": "",
"country": "",
"enhancedSANTypes": {
"dnsnames": [
"testgodaddy"
],
"dNSNames": [
"testgodaddy"
]
},
"organizationUnit": "",
"state": "",
"mailAddress": "",
"keyType": "RSA",
"bitLength": "1024",
"hashFunction": "SHA160",
"ellipticCurve": "",
"encryptedChallengePassword": "",
"certificateCategories": [
"Server",
]
},
"renewBefore": 0,
"autoRegenerateEnabled": false,
"regenerateBeforeInDays": 0,
"inheritedFromGroup": false,
"caSettingName": "Godaddy",
"validityInDays": 365,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"vendorSpecificDetails": {
"slotSize": "10",
"orderId": ""
},
"whiteLabelledCA": false,
"existingUuid": "",
"validityUnit": "years",
"validityUnitValue": 1,
"certificateCategory": "Server and Client",
"isAutoRenewal": false
},
"csrGenerationSource": "appviewx",
"fileIds": []
}
```


Response


```
{
 "response": {
 "resourceId": "60630a762be80b7ea8f03c06",
 "requestId": "155"
 },
 "message": "Certificate submission triggered successfully.",
 "appStatusCode": null,
 "tags": {},
 "headers": null
}
```


Google

Google Request Objects

Google caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Google caConnectorInfo (continued)

Name	Description
	Constraint: The value should be **Google**.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
issuerName	(Mandatory) Location of the Issuer configured at the CA end. **Type**: String
issuerLocation	(Mandatory) Parameters that are necessary for generating the CSR. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Google CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Google genericFields

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Google caConnectorInfo (continued)

Name	Description
vendorSpecificDetails	(Optional) Data specific to the Digicert vendor. **Type**: Google vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified. **Type**: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

Google CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Google CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
EmailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Google CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters is dNSNames.
dNSNames	(Optional) List of subject alternative names for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Google CSR Parameters (continued)

Name	Description
enhancedSANTypes	**Type**: Array of String

Google genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Google vendorSpecificDetails

Name	Description
certificateId	(Optional) Unique name of the certificate maintained in Google CA. **Type**: String **Constraint**: If there's no value entered, it will be filled with common name and the current timestamp.

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"certificateAuthority": "Google",
"autoRegenerateEnabled": false,
"caSettingName": "Google",
"issuerLocation": "us-east1",
"issuerName": "AppViewX-Demo",
"description": "",
"csrParameters": {
"commonName": "testgooglecertificate",
"subjectAlternativeNames": [
"dNSNames"
],
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"postalCode": "",
"certificateCategories": [
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testgooglecertificate"
]
}
},
"genericFields": {
"device_name_Google": "",
"vs_ip_Google": ""
},
"vendorSpecificDetails": {
"certificateId": ""
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
},
"validityUnitValue": "1",
"validityInDays": 365,
"validityUnit": "years"
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "148"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


InCommon

InCommon Request Objects

InCommon caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **InCommon**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

InCommon caConnectorInfo (continued)

Name	Description
	Constraint: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

InCommon caConnectorInfo (continued)

Name	Description
	Type: InCommon CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: InCommon genericFields
vendorSpecificDetails	(Optional) Data specific to the InCommon vendor. **Type**: InCommon vendorSpecificDetails
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer

InCommon CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

InCommon CSR Parameters (continued)

Name	Description
	Constraint: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

InCommon genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

InCommon genericFields (continued)

Name	Description
	Type: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

InCommon vendorSpecificDetails

Name	Description
serverType	(Mandatory) The server category to which the certificate is requested, such as AOL. **Type**: String

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "InCommon",
 "isAutoRenewal": "false",
"autoRegenerateEnabled": true,
"regenerateBeforeInDays": "30",
"caSettingName": "Incommon_test_ca",
"certificateType": "EliteSSL Certificate",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"hashFunction": "SHA256",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Client"],
"ellipticCurve": "",
"enhancedSANTypes":
"dNSNames": []
}
},
"genericFields": {
"device_name_InCommon": "test_device",
"vs_ip_InCommon": "192.168.142.162"
},
"vendorSpecificDetails": {
"serverType": "AOL"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response":
{
"resourceId": "5f47b29938c8c041c2c7096b",
"requestId": "112
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Let’s Encrypt

Lets Encrypt Request Objects

Lets Encrypt caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Lets Encrypt**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Lets Encrypt caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: LetsEncrypt CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: LetsEncrypt genericFields
vendorSpecificDetails	(Optional) Data specific to the LetsEncrypt vendor. **Type**: LetsEncrypt vendorSpecificDetails
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

Lets Encrypt CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Lets Encrypt CSR Parameters (continued)

Name	Description
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Lets Encrypt CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Lets Encrypt CSR Parameters (continued)

Name	Description
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames	(Optional) List of subject alternative names for the certificate.
`enhancedSANTypes`	**Type**: Array of String

Lets Encrypt genericFields

Name	Description
device_name_LetsEncrypt	(Optional) Server device name for which certificate is requested. **Type**: String
vs_ip_LetsEncrypt	(Optional) Server IP address for which certificate is requested. **Type**: String
f5_device	(Optional) F5 device name/IP address. **Type**: String
data_group_name	(Optional) Data group name. **Type**: String
infoblox_device	(Optional) Infoblox device name/IP address. **Type**: String
validation_ip	(Optional) Validation IP address. **Type**: String

Lets Encrypt vendorSpecificDetails

Name	Description
challengeType	(Mandatory) The challenge validation type. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Lets Encrypt vendorSpecificDetails (continued)

Name	Description
	Possible values: DNS or HTTP.

Sample Request/Response

Request Payload


```
{
 "csrGenerationSource": "appviewx",
 "caConnectorInfo": {
 "certificateAuthority": "LetsEncrypt",
 "isAutoRenewal": "false",
 "autoRegenerateEnabled": true,
 "regenerateBeforeInDays": "30",
 "caSettingName": "LetsEncrypt",
 "description": "",
 "csrParameters": {
 "commonName": "testcert.testdomain.net",
 "hashFunction": "SHA256",
 "keyType": "RSA",
 "bitLength": "4096",
 "certificateCategories": ["Server"],
 "ellipticCurve": "",
 "enhancedSANTypes": {
 "dNSNames": ["test.lab.appviewx.net"]
 }
 },
 "genericFields": {
 "device_name_LetsEncrypt": "",
 "vs_ip_LetsEncrypt": "",
 "f5_device": "",
 "data_group_name": "",
 "infoblox_device": "",
 "validation_ip": ""
 },
 "vendorSpecificDetails": {
 "challengeType": "DNS"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
},
"validityInDays": 90
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f510caa70040d33314f13d7",
"requestId": "204"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Microsoft Enterprise

Microsoft Enterprise Request Objects

Microsoft Enterprise caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Microsoft Enterprise**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise caConnectorInfo (continued)

Name	Description
	Constraint: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Microsoft Enterprise CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Microsoft Enterprise genericFields

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise caConnectorInfo (continued)

Name	Description
vendorSpecificDetails	(Optional) Data specific to the Microsoft Enterprise vendor. **Type**: Microsoft Enterprise vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String

Microsoft Enterprise CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
EmailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise CSR Parameters (continued)

Name	Description
	Type: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, directoryNames, rfc822Names, registeredIDs, uniformResourceIdentifiers, and otherNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
directoryNames `enhancedSANTypes`	(Optional) List of Directory names as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid directory name.
rfc822Names `enhancedSANTypes`	(Optional) List of mail addresses as subject alternative names for the certificate. **Type**: Array of String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise CSR Parameters (continued)

Name	Description
	Constraint: It should be a valid mail address.
registeredIDs enhancedSANTypes	(Optional) List of registered ids as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid registered id.
uniformResourceIdentifiers enhancedSANTypes	(Optional) List of URI as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid URI.
otherNames enhancedSANTypes	(Optional) List of other names as as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid name.

Microsoft Enterprise genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Enterprise vendorSpecificDetails

Name	Description
templateName	(Mandatory) Template name to issue the certificate with. **Type**: String

MS Enterprise enhancedSANTypes

Name	Mandatory	Description	Field Type	Constraints
dNSNames	No	List of Subject Alternative names for the Certificate.	Array of String	Should be a valid domain name.
iPAddresses	No	IP addresses to be considered as Subject Alternative Names.	Array of String	Must be valid ip addresses.
directoryNames	No	List of Directory names as Subject Alternative names for the Certificate.	Array of String	Should be a valid directory name.
rfc822Names	No	List of mail addresses as Subject Alternative names for the Certificate.	Array of String	Should be a valid mail address.
registeredIDs	No	List of registered ids as Subject Alternative names for the Certificate.	Array of String	Should be a valid registered id.
uniformResourceIdentifiers	No	List of URI as Subject Alternative names for the Certificate.	Array of String	Should be a valid URI.
otherNames	No	List of other names as Subject Alternative names for the Certificate.	Array of String	Should be a valid other name.

Sample Request/Response

Sample Request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Microsoft Enterprise",
"isAutoRenewal": false,
"autoRegenerateEnabled": false,
"caSettingName": "MS_ENT",
"certificateType": "",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
"hashFunction": "SHA256",
"encryptedChallengePassword": "QWRtaW5AMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
"Server"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testmscert.appviewx.com"
]
}
},
"genericFields": {
"device_name_Microsoft Enterprise": "",
"vs_ip_Microsoft Enterprise": ""
},
"vendorSpecificDetails": {
"templateName": "ServerCertificate"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
}
},
"certificateGroup": {
"name": "Default"
}
}
```

Sample Response

```
{
 "response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "150"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```

Microsoft Standalone

Microsoft Standalone Request Objects

Microsoft Standalone caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone caConnectorInfo (continued)

Name	Description
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Microsoft Standalone CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Microsoft Standalone genericFields
name	(Optional) Name for the CA connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone caConnectorInfo (continued)

Name	Description
	Type: String

Microsoft Standalone CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone CSR Parameters (continued)

Name	Description
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
EmailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone CSR Parameters (continued)

Name	Description
	Recommendation: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames, iPAddresses, directoryNames, rfc822Names, registeredIDs, uniformResourceIdentifiers, and otherNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
directoryNames `enhancedSANTypes`	(Optional) List of Directory names as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid directory name.
rfc822Names `enhancedSANTypes`	(Optional) List of mail addresses as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid mail address .
registeredIDs	(Optional) List of registered ids as subject alternative names for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Microsoft Standalone CSR Parameters (continued)

Name	Description
`enhancedSANTypes`	**Type**: Array of String **Constraint**: It should be a valid registered id.
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) List of URI as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid URI.
otherNames `enhancedSANTypes`	(Optional) List of other names as as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid name.

Microsoft Standalone genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Microsoft Standalone",
"isAutoRenewal": false,
"autoRegenerateEnabled": false,
"caSettingName": "MS_STD",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "AppViewX",
"locality": "Texas",
"state": "Texas",
"country": "US",
"mailAddress": "test@appviewx.com",
"hashFunction": "SHA256",
"encryptedChallengePassword": "QWRtaW5AMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": [
"Server",
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [
"testmscert.appviewx.com"
]
}
},
"genericFields": {
"device_name_Microsoft Standalone": "",
"vs_ip_Microsoft Standalone": ""
}
},
"certificateGroup": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e5c2e70040d33314f0e9d",
"requestId": "151"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


OpenTrust

OpenTrust Request Objects

Opentrust caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Digicert**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Opentrust caConnectorInfo (continued)

Name	Description
	Type: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Opentrust CSR Parameters
vendorSpecificDetails	(Mandatory) Data specific to the Opentrust vendor. **Type**: Opentrust vendorSpecificDetails
name	(Optional) Name for the CA connector. **Type**: String
certificateProfileName	(Mandatory) Name of the certificate profile configured in the CA portal.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Opentrust CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Opentrust CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Opentrust CSR Parameters (continued)

Name	Description
	Possible value: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames and iPAddresses.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String
iPAddresses `enhancedSANTypes`	(Optional) List of IP address to be considered as subject alternative names. **Type**: Array of String
uniformResourceIdentifiers `enhancedSANTypes`	(Optional) List of URI as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid URI.
rfc822Names `enhancedSANTypes`	(Optional) List of mail addresses as subject alternative names for the certificate. **Type**: Array of String **Constraint**: It should be a valid mail address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Opentrust vendorSpecificDetails

Name	Description
formFields	(Mandatory) Certificate parameters that are configured in the chosen certificate profile. **Type**: List of objects - formFields **Constraint**: CA settings must be saved after choosing the required certificate profile.
commonName1 formFields	Mandatory constraint depends on the profile configuration in the CA portal. Fully qualified domain name (FQDN) of the server for which certificate is requested. (Parameters can be identified in the CA portal or the certificate enrollment page in the AppViewX UI.) **Type**: String **Note:** Multiple parameters may be configured in the Certificate Management Profile in the OpenTrust CA portal. The parameter mentioned is a sample.

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "OpenTrust",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "OpenTrust",
"description": "Test certificate",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"certificateCategories": ["Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"vendorSpecificDetails": {
"formFields": {
"commonName1": "testcertot.appviewx.net",
"subjectAltNameDNS1": "testcertot1.appviewx.net"
}
},
"certificateProfileName": "server"
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "606357ec14974147f02c53ec",
"requestId": "119"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sectigo

Sectigo Request Objects

Sectigo caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Possible Values**: Sectigo, Comodo Certificate Manager
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sectigo caConnectorInfo (continued)

Name	Description
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Sectigo CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Sectigo genericFields
vendorSpecificDetails	(Optional) Data specific to the Sectigo vendor. **Type**: Sectigo vendorSpecificDetails
validityUnitValue	(Mandatory) Specifies the number of days, months, or years of validity for the CA based on the value in the "validityUnit." For example, if the expected validity is 1 year and "validityUnit" is months, then the "validityUnitValue" should be 12. **Type**: Integer **Constraint**: If the validityUnit is not provided, then the validityUnitValue must be provided in days.
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
validityUnit	(Optional) Specifies the unit in which the "validityUnitValue" is specified.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sectigo caConnectorInfo (continued)

Name	Description
	Type: Integer **Constraint**: Possible values are days, months, or years.
name	(Optional) Name for the CA connector. **Type**: String

Sectigo CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sectigo CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Sectigo genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sectigo genericFields (continued)

Name	Description
	Constraint: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sectigo vendorSpecificDetails

Name	Description
serverType	(Mandatory) The server category to which the certificate is requested, such as AOL. **Type**: String

Sample Request/Response

Request Payload


```
{
 "csrGenerationSource": "appviewx",
"caConnectorInfo":
{
"certificateAuthority": "Sectigo",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
 "caSettingName": "Sectigo_Test",
"certificateType": "EliteSSL Certificate",
 "description": "",
"csrParameters":
{
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"commonName": "testcert2n.ams1907.com",
"hashFunction": "SHA256",
"keyType": "RSA",
 "bitLength": "2048",
 "certificateCategories":
 [
"Client"
],
 "ellipticCurve": "",
 "enhancedSANTypes":
 {
"dNSNames": []
 }
 },
 "genericFields":
{
"device_name_Sectigo": "TestDevice",
"vs_ip_Sectigo": "192.168.192.168"
},
 "vendorSpecificDetails":
{
"serverType": "Apache-SSL (Ben-SSL, not Stronghold)"
},
 "validityUnitValue": "365",
"validityInDays": "365",
"validityUnit": "days"
},
 "certificateGroup":
{
 "name": "Default"
},
"certificateFormat":
{
 "format": "PEM",
"password": ""
 }
 }
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response


```
{
"response":
{
 "resourceId": "5e98047171eee023092ba006",
"requestId": "242"
 },
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Symantec

Symantec Request Objects

Symantec caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Symantec**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Symantec caConnectorInfo (continued)

Name	Description
	Constraint: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field. If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Symantec CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Symantec genericFields
vendorSpecificDetails	(Optional) Data specific to the Symantec vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Symantec caConnectorInfo (continued)

Name	Description
	Type: Symantec vendorSpecificDetails
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

Symantec CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as ‘Strict.’
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Symantec CSR Parameters (continued)

Name	Description
	Constraint: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String **Type**: String
encryptedChallengePassword	(Mandatory) Base64 encoded challenge password.
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Symantec CSR Parameters (continued)

Name	Description
	Type: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate **Type**: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameter is dNSNames.
dNSNames	(Optional) List of subject alternative names for the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Symantec CSR Parameters (continued)

Name	Description
enhancedSANTypes	**Type**: Array of String

Symantec genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Symantec vendorSpecificDetails

Name	Description
serverType	(Optional) The server category to which the certificate is requested, such as Redhat. **Type**: String

Sample Request/Response

Request Payload

```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Symantec",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"caSettingName": "Symantec",
"certificateType": "Standard",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"locality": "Plano",
"state": "Texas",
"country": "US",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"encryptedChallengePassword": "QXBwVmlld1hAMTIz",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
"genericFields": {
"device_name_Symantec": "test_device",
"vs_ip_Symantec": "xxx.xxx.xxx.xxx"
},
"vendorSpecificDetails": {
"serverType": "Red Hat"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"resourceId": "5f4fe53c70040d33314f122d",
"requestId": "190"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Trustwave

Trustwave Request Objects

Trustwave caConnectorInfo

Name	Description
certificateAuthority	(Mandatory) Name of the certificate authority that issues the certificate. **Type**: String **Constraint**: The value should be **Trustwave**.
isAutoRenewal	(Optional) Determines whether the certificate will be renewed before its expiration date. If enabled (true), renewal is initiated before the expiry date, following the specified number of days in "renewBefore." **Type**: Boolean **Constraint**: The value should be disabled (false) if autoRegenerateEnabled is true.
renewBefore	(Optional) Specifies the number of days prior to expiration when the renewal request should be triggered. **Type**: Integer **Constraint**: The value must be provided if isAutoRenewal is true.
autoRegenerateEnabled	(Optional) Determines whether the certificate will be regenerated before its expiration date, as indicated by the "regenerateBeforeInDays" field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Trustwave caConnectorInfo (continued)

Name	Description
	If enabled (true), regeneration occurs before expiry, according to the specified number of days in "regenerateBeforeInDays." **Type**: Boolean **Constraint**: The value should be disabled (false) if isAutoRenewal is true.
regenerateBeforeInDays	(Optional) Specifies the number of days prior to expiration when the regenerate request should be triggered. **Type**: Integer
caSettingName	(Mandatory) Name of the CASetting created in AppViewX for the chosen certificate authority. **Type**: String
certificateType	(Mandatory) Name of the certificate product offered by the certificate authority. **Type**: String
description	(Optional) Information about the certificate. **Type**: String
csrParameters	(Optional) Parameters required for generating a CSR. **Type**: Trustwave CSR Parameters
genericFields	(Optional) Custom fields configured for the CA/customer. **Type**: Trustwave genericFields
validityInDays	(Optional) Specifies the validity in days. **Type**: Integer
name	(Optional) Name for the CA connector. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Trustwave CSR Parameters

Name	Description
commonName	(Mandatory) A fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String **Constraint**: It must be compliant with the common name specified in the policy, if the policy is set as 'Strict.' **Note:** commonName field is optional for Code Signing certificates.
organization	(Optional) Legal name of the organization. **Type**: String **Constraint**: Default value - the value configured in the policy.
organizationUnit	(Optional) Division or department of the organization handling the certificate. **Type**: String **Constraint**: Default value - the value configured in the policy.
streetAddress	(Optional) Street name where the organization is located. **Type**: String
locality	(Optional) City where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.
state	(Optional) State or region where the organization is located. The value should not be abbreviated. **Type**: String **Constraint**: Default value - the value configured in the policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Trustwave CSR Parameters (continued)

Name	Description
country	(Optional) A two-letter code for the country where the organization is located. **Type**: String **Constraint**: Default value - the value configured in the policy.
postalCode	(Optional) Postal code for the organization address. **Type**: String
mailAddress	(Optional) Email address of the organization. **Type**: String
hashFunction	(Optional) The hash function to be used in the Certificate, e.g. SHA160. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
keyType	(Optional) The algorithm to be used for key generation, e.g. RSA, DSA, or EC. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy.
bitLength	(Optional) The bit length for the key is dependent on the key type chosen. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
certificateCategories	(Mandatory) Purpose or intended use of the generated certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Trustwave CSR Parameters (continued)

Name	Description
	Type: Array of string **Possible value**: Server, Client, Code Signing, and Email **Recommendation**: Assign only one of the possible values as the input. For example, if intended certificate category is client, set this parameter to **Client**.
ellipticCurve	(Optional) If the keyType chosen is EC, then the ellipticCurve must be specified depending on the bit length selected. It should be chosen from the possible values configured in the certificate policy. **Type**: String **Constraint**: Default value - the first value will be chosen from the policy
enhancedSANTypes	(Optional) The subject alternative names (SAN) for the certificate. The sub-parameters are dNSNames.
dNSNames `enhancedSANTypes`	(Optional) List of subject alternative names for the certificate. **Type**: Array of String

Trustwave genericFields

Name	Description
device_name_<certificateAuthority>	(Optional) Server device name for which certificate is requested. **Type**: String **Constraint**: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.
vs_ip_<certificateAuthority>	(Optional) Server IP address for which certificate is requested. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Trustwave genericFields (continued)

Name	Description
	Constraint: The <certificateAuthority> has to be replaced with the value provided in the "certificateAuthority" field.

Sample Request/Response

Request Payload


```
{
"csrGenerationSource": "appviewx",
"caConnectorInfo": {
"certificateAuthority": "Trustwave",
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"caSettingName": "trustwave",
"certificateType": "SecureTrust Organization Validation",
"description": "",
"csrParameters": {
"commonName": "testcert.testdomain.com",
"organization": "AppViewX",
"organizationUnit": "PE",
"streetAddress": "Park Street",
"locality": "Plano",
"state": "Texas",
"country": "US",
"postalCode": "75093",
"mailAddress": "test@test.com",
"hashFunction": "SHA256",
"keyType": "RSA",
"bitLength": "2048",
"certificateCategories": ["Client"],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": []
}
},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"genericFields": {
"device_name_Trustwave": "test_device",
"vs_ip_Trustwave": "xxx.xxx.xxx.xxx"
},
"validityInDays": 365
},
"certificateGroup": {
"name": "Default"
}
}
```


Response


```
{
"response": {
"resourceId": "5f4e934570040d33314f0f1d",
"requestId": "151"
},
"message": "Certificate submission triggered successfully.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Common Payload Objects

genericFields

Name	Mandatory	Description	Field Type	Constraints
device_name_<certificateAuthority>	No	Device name of the Server for which certificate is requested.	String	In the field name, <certificateAuthority> has to be replaced by the value provided for certificateAuthority in caConnectorInfo.
vs_ip_<certificateAuthority>	No	IP address of the server for which certificate is requested.	String	In the field name, <certificateAuthority> has to be replaced by the value provided for certificateAuthority in caConnectorInfo.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Create a Certificate in Sync mode

The API sends a request for certificate creation in the sync mode, where the certificate is generated immediately and returned in the response. The request payload differs based on the Certificate Authority (CA) for which enrollment or creation is being requested. Unlike async APIs, two parameters, **isSync** and **ttl**, stand out. When **isSync** (Sync Mode) is set to **true**, it overrides the certificate request approval policy to create a new certificate. These parameters are applicable to all CAs mentioned in the async APIs.

Before you begin

- The CA must configured in AppViewX from the Certificate Authority page.
- The user should have the ACF permission to submit certificates within the specified certificate's category.
- The group associated with the certificate must have RW permission.
- Connectivity to the CA via the chosen setting should be working correctly.
- A certificate group should be created and associated with the policy. If not, the certificate will be created under the Default group.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/create
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/create?gwsource=external&isSync=true&ttl=300` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
isSync *Query*	Determines whether use the sync or async APIs. If **true** - use sync and **false** - use async API. The default value is **FALSE**. **Type**: Boolean **Constraint**: Value of the parameter should be **true** or **false**.
ttl *Query*	(Mandatry) The time to live (**ttl**) is a query parameter. If the total time taken surpasses this value, the response will indicate that the request is still in progress. On the other hand, if the operation completes successfully within the TTL, the response will indicate success. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: It must be a positive value.
Payload	Contains all the parameters to be sent in the request body for the post request.
Body	**Type**: Payload

Payload

Payload

Name	Description
csrGenerationSource	(Optional) Specifies where the CSR is to be generated. **Type**: **Possible values:**: AppViewX, Endpoint, HSM, uploadCSR. The default value is **AppViewX**
caConnectorInfo	(Mandatory) Details related to the certificate authority (CA) and the CSR parameters. **Type**: Any of the following data: • Amazon caConnectorInfo • AppViewX caConnectorInfo • DigiCert caConnectorInfo • EJBCA caConnectorInfo • Entrust caConnectorInfo • EntrustMPKI caConnectorInfo • GlobalSign caConnectorInfo • GoDaddy caConnectorInfo • Google caConnectorInfo • InCommon caConnectorInfo • LetsEncrypt caConnectorInfo • Microsoft Enterprise caConnectorInfo • Microsoft Standalone caConnectorInfo • OpenTrust caConnectorInfo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	• Sectigo caConnectorInfo • Symantec caConnectorInfo • Trustwave caConnectorInfo
certificateGroup	Specifies the group (category) to which the newly created certificate should be assigned. **Type**: certificateGroup **Constraint**: Default certificate Group is "**Default**".
deviceDetails	(Optional) Information about the device or endpoint where the Certificate Signing Request (CSR) will be generated. **Type**: deviceDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **Endpoint**.
certificateHSMDetails	(Optional) Information about the Hardware Security Module (HSM) device. **Type**: certificateHSMDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **HSM**.
uploadCsrDetails	(Optional) Information about the CSR. **Type**: uploadCsrDetails **Constraint**: It is **mandatory** if **csrGenerationSource** is **uploadCSR**.
certificateFormat	(Mandatory) Certificate download format details **Type**: certificateFormat

certificateGroup

Name	Mandatory
name	(Optional) Specifies the group under which the created certificate needs to be tagged. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateGroup (continued)

Name	Mandatory
	Constraint: The certificate group must be present in AppViewX.

deviceDetails

Name	Mandatory
category	(Mandatory) Specifies the device category **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor	(Mandatory) Name of the vendor for the chosen device. For example, **Apache** is a vendor for **Server** category. **Type**: String
deviceName	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
csrFileName	(Mandatory) Name of the CSR file that is generated in the device. **Type**: String
keyFileName	(Mandatory) Name of the key file that is generated in the device. **Type**: String
attributes	(Optional) Additional attributes for the chosen device as mentioned the sub-attributes - csrLocation, tenant, and partition. **Type**:
csrLocation attributes	(Optional) The location within the device where the CSR is generated. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Server** and the **deviceDetails.vendor** is **Tomcat**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

deviceDetails (continued)

Name	Mandatory
tenant attributes	(Optional) Name of the partition within the AVI device. **Type**: String
partition attributes	(Optional) Name of the partition within the device. **Type**: String **Constraint**: It is **mandatory** when **deviceDetails.category** is **Friewall** and the **deviceDetails.vendor** is **Fortinet**.

certificateHSMDetails

Name	Mandatory
type	(Mandatory) Type of the HSM device. **Type**: String **Possible values**: ADC and HSM.
keyReference	(Mandatory) Reference name for the key that is mapped by the HSM device. **Type**: String
hsmSettings	(Mandatory) Configuration details for the HSM device. Contains the sub-parameters vendorType and vendorSpecificSettings **Type**: List <String>
vendorTypehsmSettings	(Mandatory) Category of the vendor. **Type**: String **Possible values**: Safenet, Thales, and Fortanix.
vendorSpecificSettingshsmSettings	(Mandatory) Settings related to HSM vendor. Contains the sub-parameter moduleId

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateHSMDetails (continued)

Name	Mandatory
	Type: String
moduleId `hsmSettings. vendorSpecificSettings`	(Optional) The module id. **Type**: String **Constraints**: Applicable if **hsmSettings.vendorType** is **Thales**.
vendor	(Mandatory) The name of the vendor for the chosen device e.g., F5. **Type**: String
deviceName	(Mandatory) The name of the device as per AppViewX Device Inventory. **Type**: String

uploadCsrDetails

Name	Mandatory
category	(Mandatory) Certificate category **Type**: String **Possible values**: Server, Client, and Code Signing
csrContent	(Mandatory) The CSR content for certificate enrollment request **Type**: String

certificateFormat

Name	Mandatory
format	(Mandatory) Certificate download format. Refer to the Possible values for Certificate Download Format table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateFormat (continued)

Name	Mandatory
	Type: String
password	(Optional) The field is mandatory for some parameters (refer to the table below). **Type**: String

Possible values for Certificate Download Format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.p12	P12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body params:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
resourceId response	Identifier of the certificate record that has been created (the resourceId in the above request can be found using the search API using commonName, serial No. or other search parameters). **Type**: String
requestId response	Open work order request ID. **Type**: String
certificateContent response	Content of certificate in Base64 encoded format. **Type**: String
encodedFormat response	Certificate content encoded format. **Type**: String
certificateName response	Certificate name. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate submission triggered successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	INVALID_REQUEST	Invalid request specified **Remediation**: Ensure that the payload is valid.
400 Bad Request	INVALID_CSR_GEN_SOURCE	Invalid csr generation source specified. **Remediation**: Ensure that a valid value is provided for the csrGenerationSource field in the request.
400 Bad Request	INVALID_TTL_VALUE	Please provide valid integer for **ttl**. **Remediation**: Ensure the value of **ttl** in query params is an integer.
417 Expectation failed	READ_GROUP	Group is given with read permission, so cannot perform any operation. **Remediation**: Ensure that the group associated with the certificate has read write permissions for the user.
417 Expectation Failed	CERT-GEN-0055	**orderValidityUnit** and **orderValidityUnitValue** field inside **caConnectorInfo.vendorSpecificDetails** or **validityUnit** and **validityUnitValue** is mandatory **Remediation**: Ensure valid values are assigned to the mandatory fields.
417 Expectation Failed	READ_GROUP	Group is given with read permission, so cannot perform any operation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure group name entered in the payload has RW permissions.
417 Expectation Failed	FAILED	Certificate create action in progress during CSR Submission. **Remediation**: Ensure the test connection is successful.
417 Expectation Failed	FAILED	Certificate create action Failed during CSR Submission due to Unable to submit the CSR request to certificate authority.-validity_years contains an invalid value **Remediation**: Ensure that the validity in your CSR request is set to a valid number
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure the user has ACF permission to enroll/submit certificates within the specified certificate's category.
404 Expectation failed	GROUP_NOT_FOUND	Invalid group name specified. **Remediation**: Ensure that a valid value is provided for the certificateGroup section in the request.
404 Not Found	CERT-PLCY-0003	Policy information not available **Remediation**: Ensure if **Certificate Authority** mapping is available in the **Certificate Policy** of the group mentioned in the payload
404 Not Found	CERT-CA-0001	CA settings are not available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the caSettingName section in the request.

Sample Request/Response

Request Payload


```
{
"caConnectorInfo": {
"caSettingName": "",
"validityInDays": 365,
"isAutoRenewal": "true",
"renewBefore": "30",
"autoRegenerateEnabled": false,
"certificateType": "",
"csrParameters": {
"commonName": "",
"organization": "",
"organizationUnit": "",
"locality": "",
"state": "",
"country": "",
"mailAddress": "",
"encryptedChallengePassword": "",
"hashFunction": "",
"keyType": "",
"bitLength": "",
"certificateCategories": [
"Server",
"Client"
],
"ellipticCurve": "",
"enhancedSANTypes": {
"dNSNames": [],
"iPAddresses": [],
"uniformResourceIdentifiers": []
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
}
}
"genericFields": {
"device_name_Entrust": "",
"vs_ip_Entrust": "",
"type": "",
"owner_email": "",
"environment": "",
"partition": "",
"devices": "",
"sync_group": "",
"requestor": "",
"project": ""
},
"vendorSpecificDetails": {
"avx_requester_fullname":"",
"avx_requester_emailid":"",
"avx_requester_phoneno": "",
"additionalEmails": ""
},
"customAttributes": {
"attribute1": ""
}
},
"certificateGroup": {
"name": "Default"
},
"certificateFormat": {
"format": "PEM",
"password": ""
}
}
```


Response


```
{
"response": {
"resourceId": "<Certificate Object ID>",
"requestId": "<Certificate WF Request ID>",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"certificateContent": "<Encoded Certificate Content>",
"encodedFormat": "base64",
"certificateName": "<Name of the Certificate>"
},
"message": "Certificate create and download action performed successfully",
"appStatusCode": "<Error Code>",
"tags": {},
"headers": null
}
```


What's next?

Add Certificate Attributes

Download a Certificate

Download a Certificate by Format

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Renew a Certificate in Async mode

The API initiates a request to renew an existing certificate in asynchronous mode. Upon successful triggering of the renew certificate API, the response includes a resourceId. This resourceId can be utilized to trigger the search API API, retrieving the newly created certificate. Please refer to the After you are done section for steps to approve and implement the request.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA setting should be configured in AppViewX for the CA.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session ID received after login.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
resourceId	(Optional) Unique Id of the certificate. (The resourceId in the above request can be found through the search API using commonName, serialNumber or other search parameters.) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Required if the commonName and serialNumber are not specified.
commonName	(Optional) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Optional) Serial number of the certificate **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the renewal. **Type**: String **Constraint**: Value should be **Renew**
challengePassword	(Optional) Base64 encoded value of challenge password **Type**: String **Constraint**: Applicable and mandatory for Symantec Certificate Authority.
validityUnit	(Optional) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days
validityUnitValue	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit **Type**: Integer
workflowType	(Optional) To renew the certificate without executing the workflow, set this to **direct**. By default, the workflow for certificate renewal is executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Possible values**: direct

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the renewal request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Renew action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Renew action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	INVALID_REQUEST	Invalid request specified **Remediation**: Ensure that the payload is valid
400 Bad Request	VALIDATION_ERROR_0004	Invalid **serialNumber**. **Remediation**: Ensure that the **serialNumber** is entered correctly
400 Bad Request	VALIDATION_ERROR_0004	Invalid **resourceId**. : Ensure that the **resourceId** is entered correctly.
417 Expectation Failed	READ_GROUP	Group is given with read permission, so cannot perform any operation. **Remediation**: Ensure the group associated with the certificate must have RW permission for the user.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Trigger the request once the open work order for the certificate is completed.
417 Expectation Failed	CERT-CSR-0005	CSR submission failed. **Remediation**: Use the reissue option for this DigiCert certificate as the order for this certificate is still valid. If you still wish to renew, it will incur costs.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure the user has ACF permission to renew certificates within the specified certificate's category.
404 Not Found	NO_RECORDS_FOUND	No matching records found **Remediation**: Check and ensure that the values provided for **commonName**/ **serialNumber**/ **resourceId** are correct.
500 Internal Server Error	FAILED	Certificate Renew action failed during renewal submission due to CSR or private key is not available. **Remediation**: To renew, upload private key or CSR, or use regenerate option.
500 Internal Server Error	CANNOT_PERFORM_OPERATION	Cannot perform the specified operation. Probable cause: The specified action is not permitted for certificates in a **monitored** status..

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Change the status of the certificate from a **monitored** status to a **managed** status

Sample Request/Response

Request Payload


```
{
 "commonName":"testcert8g.appviewx.plus",
 "serialNumber":"0D:A9:2D:8C:90:BB:90:B0:CE:7D:6A:76:BF:70:75:81",
 "action":"Renew"
 }
```


Response


```
{
"response": {
"resourceId": "5f4faf3e70040d33314f1142",
"message": "Renew action triggered successfully.",
"requestId": "209"
},
"message": "Renew action has been triggered successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


What's next?

- Revoke a Certificate in Async mode.
- Reissue a Certificate in Async mode.

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Renew a Certificate in Sync mode

The API initiates a certificate renewal request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for certificate renewal. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Before you begin

- The user should have the ACF permission to renew certificates within the specified certificate’s category.
- The certificate to be renewed should not be in the revoked or monitored state.
- The CA connector for the certificate should be available.
- The certificate should be present in a group that has RW permission.
- There should be no open work orders available for the certificate.
- The certificate should be present in AppViewX, with either its CSR/ private key along with it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The newly renewed certificate will fall under the same group as the existing certificate.
- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/renew
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/renew?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
isSync *Query*	(Optional) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer **Constraint**: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
resourceId	(Mandatory) Mongo ID of the certificate in the AppViewX database. (It refers to the resourceId field in the create certificate response.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory. **Note:** commonName field is optional for Code Signing certificates.
serialNumber	(Mandatory) Serial number of the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
certificateFormat	(Mandatory) Certificate format and access details **Type**: certificateFormat
workflowType	(Optional) To renew the certificate without executing the workflow, set this to **direct**. By default, the workflow for certificate renewal is executed. **Type**: String **Possible values**: direct

certificateFormat

Name	Description
format	(Mandatory) Certificate downloadable format. **Type**: String **Constraint**: For the possible values for the certificate download format, click here.
password	(Mandatory) The field is mandatory for some parameters. **Type**: String **Constraint**: For the possible values for the certificate download format, click here.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Possible values for certificate download format (continued)

Certificate Extension	Value in the Payload	Password Required
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.pk12	PK12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request.
resourceId	Identifier of the certificate record that has been created. response **Type**: String
requestId	Open work order request ID. response **Type**: String
certificateContent	Content of certificate in Base64 encoded format. response **Type**: String
encodedFormat	Certificate content in encoded format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: String
certificateName	Name of the certificate. response **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Renew action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	INVALID_REQUEST	Invalid request specified. **Remediation**: Ensure that the payload is valid.
400 Bad Request	VALIDATION_ERROR_0004	Invalid **serialNumber**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the resourceId is entered correctly
400 Bad Request	VALIDATION_ERROR_0004	Invalid **resourceId** **Remediation**: Ensure that the resourceId is entered correctly
400 Bad Request	MANDATORY_FIELD_MISSING	Either **resourceId** or **commonName** & **serialNumber** are Mandatory **Remediation**: Please ensure either **resourceId** or **commonName** & **serialNumber** are entered
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - **commonName**. **Remediation**: Ensure that the **commonName** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - **serialNumber**. **Remediation**: Ensure that the **serialNumber** field is available in the request payload.
400 Bad Request	VALIDATION_ERROR_0004	Validation Failure: Field **format** does not have the expected value **Remediation**: Please ensure **format** is entered from the possible values for certificate download format.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure the user has ACF permission to renew certificates within the specified certificate's category.
404 Not Found	NO_RECORDS_FOUND	No matching records found **Remediation**: Check and ensure that the values provided for commonName/ serialNumber/ resourceId are correct
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the renew action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.
417 Expectation Failed	READ_GROUP	Group is given with read permission, so cannot perform any operation **Remediation**: Ensure the group associated with the certificate must have RW permission for the user.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Trigger the request once the open work order for the certificate is completed
417 Expectation Failed	CERT-GEN-0055	**orderValidityUnit** and **orderValidityUnitValue** field inside **caConnectorInfo.vendorSpecificDetails** or **validityUnit** and **validityUnitValue** is mandatory **Remediation**: Ensure valid values are assigned to the mandatory fields.
500 Internal Server Error	FAILED	Certificate Renew action failed during renewal submission due to CSR or private key is not available. **Remediation**: To renew, upload private key or CSR, or use regenerate option.
500 Internal Server Error	CANNOT_PERFORM_OPERATION	Cannot perform the specified operation. Probable Cause: The specified action is not permitted for certificates in a **monitored** status. **Remediation**: Change the status of the certificate from a **monitored** status to a **managed** status
500 Internal Server Error	FAILED	Certificate Renew action performed successfully but failed to download. Reason - Mandatory field is missing or invalid - **format** **Remediation**: Please ensure **certificateFormat.format** is entered in the payload.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

```
{
 "resourceId":<Mongo ID of the certificate in AppviewX Database>,
 "workflowType": "direct",
 "commonName":<Common Name of the certificate>,
 "serialNumber":<Serial Number of the certificate>,
 "certificateFormat":{
 "format" :<Cert format - check possible values table>,
 "password" :<password>
 }
 }
```

Response

```
{
    "response": {
        "certificateContent": "<Base64 encoded cert content>",
        "privateKeyContent": "",
        "resourceId": "<renewed cert ID>",
        "requestId": "<Certificate direct request ID>",
        "externalRequestId": null,
        "newCertificateUuid": "<Renewed cert UUID>",
        "newCertificateId": "<renewed cert ID>"
        "keyAlreadyExist": false,
        "tags": null
    },
    "message": "Certificate retrieved successfully from CA",
    "appStatusCode": null,
    "tags": {},
    "headers": null
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's next?

- Reissue a Certificate in Sync mode.
- Revoke a Certificate in Sync mode.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Revoke a Certificate in Async mode

The API initiates a request to revoke an existing certificate in asynchronous mode. Refer to the After you are done section to approve and implement the request.

Before you begin

Ensure the following before attempting to revoke a certificate from any CA through AppViewX:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type	(Mandatory) Specifies the nature of the data in the payload.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Value of the param should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. It is needed only in case of multi-tenant installations and can be ignored for other type of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered (e.g. external). **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
resourceId	(Optional) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Optional) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
serialNumber	(Optional) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
action	(Mandatory) Action name for the revocation. **Type**: String **Possible values**: Revoke
reason	(Mandatory) Reason for revocation. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the revoke request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Revoke action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Revoke action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open worker for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the revoke action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload

```
{
"resourceId":"5f4faf3e70040d33314f1142",
"commonName":"testcert8g.appviewx.plus",
"serialNumber":"0D:A9:2D:8C:90:BB:90:B0:CE:7D:6A:76:BF:70:75:81",
"action":"Revoke",
"reason":"Superseded"
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response


```
{
"response": {
 "resourceId": "5f4faf3e70040d33314f1142",
 "message": "Revoke action triggered successfully.",
 "requestId": "216"
 },
 "message": "Revoke action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


What's next?

- Reissue a Certificate in Async mode.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Revoke a Certificate in Sync mode

The API initiates a certificate revoke request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for the certificate revoke. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Before you begin

- The user should have ACF permission to revoke certificates within the specified certificate's category.
- The certificate to be renewed should not be in the revoked or monitored state.
- The CA connector for the certificate should be available.
- The certificate should be present in a group that has RW permission.
- There should be no open work orders available for the certificate.
- The certificate should be have a CRL Distribution Point.
- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/revoke
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/revoke?gwsource=external` To understand the elements of the sample URL, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Headers
Content-Type: application/json

Input Parameters

Name	Description
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Mandatory) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer **Constraint**: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Mongo Id of the certificate in the AppViewX database. (It refers to the 'resourceId' field in the create certificate response. It can be found through the search API using commonName, serialNunmer. or other search parameters.) **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
commonName	(Mandatory) Common name of the certificate **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory. **Note:** commonName field is optional for Code Signing certificates.
serialNumber	(Mandatory) Serial number of the certificate **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
reason	(Mandatory) Reasons for revoking the certificate **Type**: String
comments	(Mandatory) Additional comments for revoking the certificate **Type**: String **Constraint**: Comments field is mandatory for some revoke reasons alone. Refer to the valid reason for CAs table below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Valid revocation reasons for CAs

Certificate Authority	Reasons	Comments Required
Entrust	Superseded	No
	Cessation of operation	No
	Affiliation changed	No
	Key compromised	Yes

Response Structure

Parameters

Name	Description
response	Contains the response attributes for the revoke request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Open work order request ID. **Type**: String
certStatus response	Status of the certificate action request. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload

```
{
 "resourceId": "5fa27b7ffee3a70235a5816d",
 "reason" :"Superseded"
 }
```

Response

```
{
 "response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certStatus": "Revoked"
 },
 "message": "Certificate Revoke action executed successfully",
 "appStatusCode": "<Error Code>",
 "tags": {},
 "headers": null
 }
```

What's next?

- Reissue a Certificate in Sync mode.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Reissue a Certificate in Async mode

The API will initiate a request to reissue an existing certificate in asynchronous mode. Upon successful triggering of the "Reissue a certificate" API, the response will include a resourceId. This resourceId can be used to trigger the search API API, retrieving the newly created certificate. Please refer to the After you are done section for steps to approve and implement the request.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To understand the elements of the sample URL, click here.
Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
userName *Header*	(Mandatory only if **sessionID** is not provided) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Mongo Id of the certificate in the AppViewX database. (It refers to the 'resourceId' field in the create certificate response. It can be found through the search API using commonName, serialNunmer. or other search parameters.) **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory. **Note:** commonName field is optional for Code Signing certificates.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
action	(Mandatory) Action name for the reissue **Type**: String **Possible values**: Reissue
reason	(Mandatory) Reason for reissue request **Type**: String
certificateFormat	(Mandatory) Certificate format and access details **Type**: certificateFormat
uploadCSRDetails	(Mandatory) Information related to the CSR

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: uploadCSRDetails

certificateFormat

Name	Description
format	(Mandatory) Certificate downloadable format. **Type**: String **Constraint**: For the possible values for the certificate download format, click here.
password	(Mandatory) The field is mandatory for some parameters. **Type**: String **Constraint**: For the possible values for the certificate download format, click here.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.pk12	PK12	Yes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Possible values for certificate download format (continued)

Certificate Extension	Value in the Payload	Password Required
.pfx	PFX	Yes
.jks	JKS	Yes

uploadCSRDetails

Name	Description
category	(Mandatory) Certificate category. **Type**: String **Constraint**: Possible values - **Server**, **Client**, or **Code Signing**.
csrContent	(Mandatory) The CSR content for certificate enrollment request **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the reissue request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Work order request Id. **Type**: String
message response	Success message - Reissue action triggered successfully. **Type**: String
message	Success message or failure description in case of error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open workOrder for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the reissue action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
"commonName":"testcert8g.appviewx.plus",
 "serialNumber":"08:BD:54:35:FD:81:AC:A4:45:2B:FC:9F:77:56:FE:2C",
 "action":"Reissue",
 "reason":"Superseded"
 }
```


Response


```
{
"response": {
"resourceId": "5f51f7312fa95059a12b0aee",
"message": "Reissue action triggered successfully.",
"requestId": "238"
},
"message": "Reissue action has been triggered successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


What's next?

- Revoke a Certificate in Async mode.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Reissue a Certificate in Sync mode

The API initiates a certificate revoke request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for the certificate reissue. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Before you begin

- The user should have ACF permission to renew certificates within the specified certificate’s category.
- The certificate to be renewed should not be in the revoked or monitored state.
- The CA connector for the certificate should be available.
- The certificate should be present in a group that has RW permission.
- There should be no open work orders available for the certificate.
- The certificate should be present in AppViewX, with either its CSR/ private key along with it.
- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/reissue
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/reissue?gwsource=external&isSync=true&ttl=300` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Mandatory) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: The value must be a positive integer.
Payload	Contains all the parameters to be sent in the request body for the put request.
Body	**Type**: Payload

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Mongo Id of the certificate in the AppViewX database. (It refers to the 'resourceId' field in the create certificate response. It can be found through the search API using commonName, serialNumber. or other search parameters.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory. **Note:** commonName field is optional for Code Signing certificates.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
reason	(Mandatory) Reasons for reissuing the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
uploadCSRDetails	(Mandatory) Information related to the CSR **Type**: uploadCSRDetails
certificateFormat	(Mandatory) Configuration for certificate download **Type**: certificateFormat

uploadCSRDetails

Name	Description
category	(Mandatory) Certificate category. **Type**: String **Constraint**: Possible values - **Server**, **Client**, or **Code Signing**.
csrContent	(Mandatory) The CSR content for certificate enrollment request **Type**: String

certificateFormat

Name	Description
format	(Mandatory) Certificate download format. **Type**: String **Constraint**: Refer to the possible values for certificate download format table.
password	(Mandatory) The field is mandatory for some parameters. **Type**: String **Constraint**: Refer to the possible values for certificate download format table.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.p12	P12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the reissue request.
resourceId	Identifier of the certificate record that has been created.
response	**Type**: String
requestId	Open work order request ID.
response	**Type**: String
certificateContent	Content of certificate in Base64 encoded format.
response	**Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
encodedFormat response	Certificate content encoded format. **Type**: String
certificateName response	Name of the Certificate. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Certificate reissue action performed successfully.
202 Accepted	SUCCESS	Certificate reissue action is in progress and waiting in **Awaiting Certificate Retrieval** **Remediation**: Approve the certificate request in the respective CA portal.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		sessionId is provided as header parameters.
400 Bad Request	INVALID_REQUEST	Invalid request specified **Remediation**: Ensure that the payload is valid
400 Bad Request	VALIDATION_ERROR_0004	Invalid **serialNumber**. **Remediation**: Ensure that the **serialNumber** is entered correctly
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - **commonName** **Remediation**: Please ensure **commonName** is entered in the payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - **serialNumber** **Remediation**: Please ensure **serialNumber** is entered in the payload.
400 Bad Request	VALIDATION_ERROR_0004	Invalid **resourceId**. **Remediation**: Ensure that the **resourceId** is entered correctly.
400 Bad Request	INVALID_REQUEST	Invalid **commonName** and **serialNumber** or **resourceId**. **Remediation**: Enter a valid **commonName** and **serialNumber** or **resourceId**.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - category. Probable Cause: The

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Category field is not specified within the **uploadCsrDetails** during the certificate enrollment. : Please ensure that the **Category** field is correctly provided within the **uploadCsrDetails** during the certificate enrollment.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - category. Probable Cause: The \"Category\" field is not specified within the \"uploadCsrDetails\" during the certificate enrollment. Remediation: Please ensure that the "Category" field is correctly provided within the "uploadCsrDetails" during the certificate enrollment.
400 Bad Request	FAILED	Certificate reissue action performed successfully but failed to download. Reason - Mandatory field is missing or invalid - **format** **Remediation**: Please ensure **certificateFormat.format** is entered in the payload
400 Bad Request	INVALID_TTL_VALUE	Please provide valid integer for **ttl**. **Remediation**: Eensure the value of **ttl** in query params is an integer.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure the user has ACF permission to reissue certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		within the specified certificate's category.
404 Not Found	CERT-CA-0001	CA settings are not available. **Remediation**: Ensure valid CA settings are entered in the payload.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for **commonName/ serialNumber/ resourceId** are correct.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status.
417 Expectation Failed	CERT-GEN-0002	Reissue is not supported for the certificates whose CSRs were generated with HSM ADC devices. **Remediation**: Use Regenerate option
417 Expectation Failed	READ_GROUP	Group is given with read permission, so cannot perform any operation. **Remediation**: Ensure the group associated with the certificate must have RW permission for the user.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation Failed	CERT-GEN-0055	**orderValidityUnit** and **orderValidityUnitValue** field inside **caConnectorInfo.vendorSpecificDetails** or **validityUnit** and **validityUnitValue** is mandatory **Remediation**: Ensure valid values are assigned to the mandatory fields.
500 Internal Server Error	CANNOT_PERFORM_OPERATION	Cannot perform the specified operation. Probable cause: The specified action is not permitted for certificates in a **monitored** status. **Remediation**: Change the status of the certificate from a **monitored** status to a **managed** status

Sample Request/Response

Request Payload

```
{
"resourceId": "<Mongo ID of the certificate in AppviewX Database>",
 "commonName": "<Common Name of the certificate>",
 "serialNumber": "<Serial Number of the certificate>",
 "reason": "<Reason for reissue>",
 "uploadCsrDetails": {
 "csrContent": "",
 "additionalSANValues": {
 "dNSNames": [],
 "iPAddresses": [],
 "uniformResourceIdentifiers": []
 }
 },
 "certificateFormat": {
 "format": "<Cert format - check possible values table>",
 "password": "<password>"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
}
}
```

Response

```
{
"response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certificateContent": <Encoded Certificate file>,
 "certificateName": <Name of the certificate>,
 "encodedFormat" : "base64"
 },
 "message": "Certificate Reissue action executed successfully"
 "appStatusCode": "<Error Code>",
 "tags": {},
 "headers": null
 }
```

What's next?

- Revoke a Certificate in Sync mode.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Regenerate a Certificate in Async mode

The API will initiate a request to regenerate an existing certificate in asynchronous mode. Upon successful triggering of the "Regenerate a certificate" API, the response will include a resourceId. This resourceId can be used to trigger the search API API, retrieving the newly created certificate. Please refer to the After you are done section for steps to approve and implement the request.

Before you begin

Ensure the following before attempting to regenerate certificate from any CA through AppViewX:

- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
userName *Header*	(Mandatory only if **sessionID** is not provided) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: The value must be **application/json**.
gwkey *Query*	(Mandatory) Tenant Key. This is required only for multi-tenant installations and can be disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Id of the certificate. **Type**: String **Constraint**: Required if the commonName and serialNumber are not specified.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified. **Note:** commonName field is optional for Code Signing certificates.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Required if resourceId is not specified.
action	(Mandatory) Action name for the regenerate request. **Type**: String **Constraint**: Value should be **Regenerate**.
reason	(Mandatory) Reason for regenerate request. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the regenerate request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	Work order request Id. **Type**: String
message response	Success message - Regenerate action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Regenerate action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open workOrder for the certificate is completed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the regenerate action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.
417 Expectation Failed	READ_GROUP	Group is assigned read permission, hence cannot perform any operation.
500 Internal Server Error	CANNOT_PERFORM_OPERATION	Cannot perform the specified action because it is not permitted for certificates in the **Monitored** state. **Remediation**: Change the certificate state to **Managed**.

Sample Request/Response

Request Payload


```
{
 "resourceId":"5f5641a7e74e187a7e3d5266",
 "commonName":"testcert8g.appviewx.plus",
 "serialNumber":"08:BD:54:35:FD:81:AC:A4:45:2B:FC:9F:77:56:FE:2C",
 "action":"Regenerate",
 "reason":"Key compromised"
 }
```


Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "response": {
 "resourceId": "5f56482ce74e187a7e3d52a2",
 "message": "Regenerate action triggered successfully.",
 "requestId": "237"
 },
 "message": "Regenerate action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Regenerate a Certificate in Sync mode

The API initiates a certificate regenerate request in Sync Mode, which differs from asynchronous APIs by using two distinct parameters: "isSync" and "ttl". When "isSync" is set to true, indicating Sync Mode, it bypasses the certificate request approval policy for the certificate regenerate. These parameters can be applied to all the Certificate Authorities (CAs) listed in the asynchronous APIs.

Before you begin

- The user should have ACF permission to regenerate the certificate under the associated certificate category.
- The group associated with the certificate must have RW permission.
- The certificate to be regenerated should not be in the monitored state.
- The CA connector for the certificate should be available.
- The certificate should be present in a group that has RW permission.
- There should be no open work orders available for the certificate.
- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/regenerate
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/regenerate?gwsource=external&isSync=true&ttl=300` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraint**: Required if username and password are not provided.
userName *Header*	(Mandatory only if **sessionID** is not provided) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
isSync *Query*	(Optional) The possible values are true and false. To utilize the sync API, set the value to **true** or set the value to **false** to use the async API. **Type**: Boolean **Constraint**: The value must be a boolean type: true or false.
ttl *Query*	(Optional) Time to live for a response in seconds. Default value is 300 seconds. **Type**: Integer **Constraint**: The value must be a positive integer.
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
resourceId	(Mandatory) Mongo Id of the certificate in the AppViewX database. (It refers to the 'resourceId' field in the create certificate response. It can be found through the search API using commonName, serialNumber. or other search parameters.) **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory. **Note:** commonName field is optional for Code Signing certificates.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Either resourceId or serialNumber and commonName is mandatory.
certificateFormat	(Mandatory) Configuration for downloading the certificate **Type**: certificateFormat

certificateFormat

Name	Description
format	(Mandatory) Certificate download format. **Type**: String **Constraint**: Refer to the possible values here.
password	(Mandatory) The field is mandatory for some parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateFormat (continued)

Name	Description
	Type: String **Constraint**: Refer to the possible values here.

Possible values for certificate download format

Certificate Extension	Value in the Payload	Password Required
.crt	CRT	No
.cert	CERT	No
.cer	CER	No
.pem	PEM	No
.der	DER	No
.cer	DERCER	No
.p7b	P7B	No
.p7c	P7C	No
.pk8	PK8	No
.p12	P12	Yes
.pfx	PFX	Yes
.jks	JKS	Yes

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the regenerate request.
resourceId	Identifier of the certificate record that has been created.
response	**Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
requestId response	Open work order request ID. **Type**: String
certificateContent response	Content of certificate in Base64 encoded format. **Type**: String
encodedFormat response	Certificate content encoded format. **Type**: String
certificateName response	Name of the Certificate. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 OK	null	Certificate regenerate action performed successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		sessionId is provided as header parameters.
400 Bad Request	INVALID_REQUEST	Invalid request specified **Remediation**: Ensure that the payload is valid
400 Bad Request	VALIDATION_ERROR_0004	Invalid **serialNumber**. **Remediation**: Ensure that the **serialNumber** is entered correctly
400 Bad Request	VALIDATION_ERROR_0004	Invalid **resourceId**. **Remediation**: Ensure that the **resourceId** is entered correctly.
400 Bad Request	MANDATORY_FIELD_MISSING	Either **resourceId** or **commonName** & **serialNumber** are Mandatory **Remediation**: Please ensure either **resourceId** or **commonName** & **serialNumber** are entered
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - **commonName** **Remediation**: Please ensure **commonName** is entered in the payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - **serialNumber** **Remediation**: Please ensure **serialNumber** is entered in the payload.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
400 Bad Request	VALIDATION_ERROR_0004	Validation Failure: Field **format** does not have the expected value. **Remediation**: Please ensure **format** is entered from the possible values for certificate download format.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure the user has ACF permission to reissue certificates within the specified certificate's category.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for **commonName**/ **serialNumber**/ **resourceId** are correct.
417 Expectation Failed	READ_GROUP	Group is given with read permission, so cannot perform any operation. **Remediation**: Ensure the group associated with the certificate must have RW permission for the user.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.
500 Internal Server Error	CANNOT_PERFORM_OPERATION	Cannot perform the specified operation. Probable cause: The specified action

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		is not permitted for certificates in a **monitored** status. **Remediation**: Change the status of the certificate from a **monitored** status to a **managed** status
500 Internal Server Error	FAILED	Certificate regenerate action performed successfully but failed to download. Reason - Mandatory field is missing or invalid - **format** **Remediation**: Please ensure **certificateFormat.format** is entered in the payload
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

```
{
 "resourceId":<Mongo ID of the certificate in AppviewX Database>,
 "commonName":<Common Name of the certificate>,
 "serialNumber":<Serial Number of the certificate>,
 "certificateFormat":{
 "format" :<Cert format - check possible values table>,
 "password" :<password>
 }
 }
```

Response

```
{
 "response": {
 "resourceId": "<Certificate ID>",
 "requestId": "<Certificate WF Request ID>",
 "certificateContent": <Encoded Certificate file>,
 "certificateName": <Name of the certificate>,
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"encodedFormat" : "base64"

},

"message": "Certificate Regenerate action executed successfully",

"appStatusCode": "<Error Code>",

"tags": {},

"headers": null

}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Suspend a Certificate

The API initiates a request to suspend an existing certificate. Refer to the After you are done section to approve and implement the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

Ensure the following before attempting to renew certificate from any CA through AppViewX:

- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password	(Mandatory) AppViewX login password.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Id of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
action	(Mandatory) Action to triggered with the request **Type**: String **Constraint**: Value should be **Suspend**
reason	(Mandatory) Reason for the suspend request **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the suspend certificate request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Suspend action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Suspend action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName/ serialNumber/ resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the suspend action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Sample Request/Response

Request Payload


```
{
 "resourceId":"5f5641a7e74e187a7e3d5266",
 "commonName":"testcert5d.avx.com",
 "serialNumber":"7E:94:56:98:57:F2:0E:3B",
 "action":"Suspend",
 "reason":"Superseded"
 }
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response


```
{
"response": {
 "resourceId": "5f4e5c2e70040d33314f0e9d",
 "message": "Suspend action triggered successfully.",
 "requestId": "241"
 },
 "message": "Suspend action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Reinstate a Certificate

The API initiates a request to reinstate a suspended certificate. Refer to the After you are done section to Approve and Implement the request.

Before you begin

Ensure the following before attempting to reinstate a certificate from any CA through AppViewX:

- The CA must configured in AppViewX from the Certificate Authority page.
- Connectivity to the CA via the chosen setting should be working correctly.
- Approval:
  - **Approval is not required:** Enable this mode by setting the **Certificate Requests Need Approval?** flag to false in the certificate policy.
  - **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/action
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username	(Mandatory) AppViewX login username.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if sessionId is not provided.
password	(Mandatory) AppViewX login password. *Header* **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type	(Mandatory) Specifies the nature of the data in the payload. *Header* **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource	(Mandatory) Source from which the request is triggered *Query* **Type**: String
Payload	Contains all the parameters to be sent in the request body for the put request. *Body* **Type**: Payload

Payload

Payload

Name	Description
resourceId	(Mandatory) Unique Id of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
commonName	(Mandatory) Common name of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
serialNumber	(Mandatory) Serial number of the certificate. **Type**: String **Constraint**: Common name and either resourceId or serialNumber is mandatory.
action	(Mandatory) Action name for reinstate request. **Type**: String **Possible values**: Reinstate
reason	(Mandatory) Reason for the reinstate request. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the reinstate certificate request.
resourceId response	Identifier of the certificate record that has been created. **Type**: String
requestId response	WorkOrder request Id. **Type**: String
message response	Success message - Reinstate action triggered successfully. **Type**: String
message	Success message or failure description in case of error. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reinstate action has been triggered successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName/ serialNumber/ resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - reason. **Remediation**: Ensure that the **reason** field is available in the request payload.
417 Expectation Failed	OPEN_WORK_ORDERS_FOUND	Since requested certificate's work order is in progress, cannot initiate another action. **Remediation**: Trigger the request once the open work order for the certificate is completed.
406 Not Acceptable	CERT-VWF-0006	Life cycle action is unsupported by CA or another work order is in progress or certificate belongs to read group or is in Monitored status. **Remediation**: Ensure the following: • The CA supports the reinstate action. • There is no workOrder in progress for the specified certificate. • Certificate does not belong to read only group. • Certificate is not in the monitored status.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload


```
{
 "resourceId":"5f4faf3e70040d33314f1142",
 "commonName":"testcert8g.appviewx.plus",
 "serialNumber":"0D:A9:2D:8C:90:BB:90:B0:CE:7D:6A:76:BF:70:75:81",
 "action":"Reinstate",
 "reason":"Test"
 }
```


Response


```
{
 "response": {
 "resourceId": "5f4faf3e70040d33314f1142",
 "message": "Reinstate action triggered successfully.",
 "requestId": "216"
 },
 "message": "Reinstate action has been triggered successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Search/Get Certificate Inventory

The API enables users to search for one or more certificates based on the provided searchable inputs. It returns full details of the matching certificate(s).

Before you begin

- The user should have the ACF permission to view the inventory associated with the searched certificate(s).
- The field referenced in the search input must already be populated for the relevant certificates.
- The group associated with the relevant certificates should at least have read access.

Request Structure

Endpoint:	/certificate/search
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/search?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session Id received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
input	(Mandatory) Search parameters such as keyword or free text search.
category input	(Optional) Specifies the certificate category A comma-separated list of multiple values can also be provided, to search for certificates across categories. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values: • Server (default) • Client • Code signing • Device • Root CA • Intermediate CA
resourceId	(Optional) Id of the certificate.
input	**Type**: String
freeSearch	(Optional) Key for free text search
input	Search will be performed on all cert fields based on the free text input provided.
	Type: String
keywordSearch	(Optional) Search by certificate attributes based on the predefined key words.
input	**Type**: String
subject:o	(Optional) Subject organization name
input. keywordSearch	**Type**: String
subject:ou	(Optional) Subject organization unit
input. keywordSearch	**Type**: String
subject:cn	(Optional) Subject common name
input. keywordSearch	**Type**: String
subject:l	(Optional) Subject location
input. keywordSearch	**Type**: String
subject:st	(Optional) Subject state

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
input. keywordSearch	**Type**: String
subject:c	(Optional) Subject country
input. keywordSearch	**Type**: String
certversion	(Optional) Certificate version
input. keywordSearch	**Type**: String
certserialno	(Optional) Certificate serial number
input. keywordSearch	**Type**: String
	Constraint: Serial number of the certificate to be specified in the same format as in example- 1C:DB:14:3D:5C:98:EC:00:D0:C1:D1:63:78:B4:AA:42
certissuer	(Optional) Issuer common name
input. keywordSearch	**Type**: String
certstatus	(Optional) Certificate status
input. keywordSearch	**Type**: String
	Possible values: Managed, New Certificate, Monitored, Discovered
certgroup	(Optional) Certificate group.
input. keywordSearch	**Type**: String
expirydate	(Optional) Certificate expiry date in the MM/DD/YYYY format
input. keywordSearch	For example, 03/26/2022
	Type: String
expiryyear	(Optional) Certificate expiry year in the YYYY format
input. keywordSearch	For example, 2022

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
expirymonth input. keywordSearch	(Optional) Certificate expiry month in the MM format For example, 03 **Type**: String
discoverysource input. keywordSearch	(Optional) Discovery source for the relevant certificates For example, the device name or the CA setting name If a CA setting is to be specified, it should be entered in the following format: **<<CA name>>::<<CA setting name>>**. For example, **EJBCA:: Setting1**. **Type**: String
ca input. keywordSearch	(Optional) Certificate Authority name **Type**: String
application input. keywordSearch	(Optional) CA name / Auto-enrollment protocol name / device vendor name **Type**: String **Constraint**: This input is applicable only for certificates that were discovered from a CA/a device and certificates that were enrolled using auto enrollment protocols. **Possible values for auto enrollment protocols**: SCEP, EST, ACME, SCEP_MS_INTUNE
issuer input. keywordSearch	(Optional) Issuer common name **Type**: String **Constraint**: Ensure that the entered value is obtained from the AppViewX certificate inventory or the certificate data, so a discrepancy/mismatch can be avoided.
hash	(Optional) Hash function

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
input. keywordSearch	**Type**: String **Possible values**: SHA160, SHA224, SHA256, SHA384, SHA512
key	(Optional) Key type
input. keywordSearch	**Type**: String **Possible values**: RSA, EC, DSA
keylength	(Optional) Bit length depending on the key type chosen
input. keywordSearch	Input value to be obtained from the defined CA policy. **Type**: String
caSettings	(Optional) CA setting name
input. keywordSearch	Input value to be obtained from the defined CA policy. **Type**: String
ellipticcurve	(Optional) Elliptic curve name
input. keywordSearch	Input value to be obtained from the defined CA policy. **Type**: String
filter	(Mandatory) Pagination and sort parameters for the search
start	(Optional) Start index from which the response has to be displayed
filter	For example, if the search results must skip the first 100 and show results from value no.101, the value of this parameter will be **101**. **Type**: Integer **Default value**: 0

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
max filter	(Optional) The number of entries from the start index to be displayed E.g., if the response is expected to have skipped the first 100 and show the next 50, then the start index has to be 101 and max has to be 50. For example, if the search results must display 50 values from the start index, the value of this parameter will be **50**. **Type**: Integer **Default value**: 100
sortOrder filter	(Optional) Sorting order for the search results **Type**: String **Possible**: asc (default), desc
sortColumn filter	(Optional) Column name for sorting **Type**: String **Default value**: _id

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes
response response	Contains the inventory response attributes
objects response.response	Certificate metadata **Type**: Array of Certificate json
totalRecords	Total number of records matching the search criteria

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
`response.response`	**Type**: String
obtainedRecords `response.response`	Number of records fetched for the query **Type**: String
obtainedRecordRange `response.response`	Index of the records fetched
start `response.response.obtainedRecordRange`	Start index of the fetched records **Type**: String
end `response.response.obtainedRecordRange`	End index of the fetched records **Type**: String
message `response`	Success or failure message **Type**: String
message	If matching records are found for the search query: **Matching results found for the given input.** If no records are available for the search query: **No matching records found for the given input.** **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Matching records are found for the search query. Success message **Matching results found for the given input.** is displayed.
404 Not Found	NA	No mtaching records found for the search query The message **No matching records found for the given input.** is displayed.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as the header parameter.
400 Bad Request	INVALID_REQUEST	Invalid sort order value **Remediation**: Ensure that a valid value is provided for `sortOrder`.
400 Bad Request	INVALID_REQUEST	Invalid request specified **Possible Causes**: • Either **filter** is not available or the filter value is invalid in the payload. • Value provided for **filter.max** is invalid. **Remediation**: Ensure that valid filter values are provided.

Sample Request/Response

Request Payload

```
{
 "input":{
 "category":"Server",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"keywordSearch" : {
"certserialno":"7E:94:56:98:57:F2:0E:3B"
}
},
"filter":{
"max":"100",
"start":"1",
"sortColumn":"commonName",
"sortOrder":"desc"
}
}
```

Response


```
{
 "response": {
 "httpStatusCode": 200,
 "response": {
 "objects": [
 {
 "commonName": "testcert5d.avx.com",
 "serialNumber": "7E:94:56:98:57:F2:0E:3B",
 "issuerCommonName": "Ejbca New Intermediate CA",
 "status": "Managed",
 "associatedObjects": [],
 "discoverySources": [],
 "subjectOrganization": "AppViewX",
 "subjectOrganizationUnit": "PE",
 "subjectLocality": "Plano",
 "subjectState": "Texas",
 "subjectCountry": "US",
 "issuerOrganization": "",
 "issuerOrganizationUnit": "",
 "issuerLocality": "",
 "issuerState": "",
 "issuerCountry": "",
 "version": "3",
 "validFrom": 1598943490000,
 "validTo": 1607583490000,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

"validFor": "90 day(s) 18 hr(s) 8 min(s)",

"keyAlgorithmAndSize": "RSA 2048",

"signatureAlgorithm": "SHA256withRSA",

"signatureHashAlgorithm": "SHA256",

"keyUsage": "DigitalSignature, NonRepudiation, KeyEncipherment",

"extendedKeyUsage": "Client Authentication(1.3.6.1.5.5.7.3.2) Server Authentication(1.3.6.1.5.5.7.3.1) ",

"basicConstraints": "Subject Type=End entity, Path Length=none",

"group": "Default",

"subjectAlternativeNames": [

"URL : http://testcert5.avx.com",

"Email address : test@testcert5.avx.com",

"DNS : testcert5.avx.com",

"IP Address : 192.168.142.162"

],

"complianceStatus": "Compliant",

"applications": [],

"expiryStatus": "Valid",

"permission": "RW",

"category": "Server",

"uuid": "4f4e23cefea2297a4e7d6b202ceee5ba47a20c89",

"certificateAuthority": "Ejbca",

"authorityKeyIdentifier": "69:15:BC:24:60:6B:73:96:8B:F3:3A:ED:C4:38:EB:58:A6:3F:4B:5B",

"subjectKeyIdentifier": "0D:31:76:0B:F1:41:AD:A6:39:6B:79:A6:43:8D:62:07:CC:F5:94:FB",

"authorityInfoAccess": [],

"certificatePolicies": [],

"crlDistributionPoints": [

"CrlDistributionPoint : [name : , url : http://192.168.12.139:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=Ejbca%20New%20Intermediate%20CA]"

],

"thumbprintAlgorithm": "SHA-1",

"thumbPrint": "9F:8E:0D:B6:A6:25:D4:05:E3:2B:5E:F7:85:1B:79:83:CB:EA:3C:DB",

"type": "Others",

"genericFields": {

"vs_ip_Ejbca": "192.168.142.162",

"device_name_Ejbca": "test_device"

},

"csrGenerationSource": "appviewx",

"newConnectors": [],

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

"csrAvailable": true,

"autoRenewDate": "",

"missingParamsForAutoRenew": "CSR parameters are available for certificate renewal",

"suspendedCertificate": false,

"mailAddress": "test@test.com",

"streetAddress": "",

"postalCode": "",

"requestIds": [

"R147",

"R241"

],

"publicKey":

"30:82:01:0A:02:82:01:01:00:8B:64:08:1A:2B:40:B9:2F:7C:48:65:78:98:B3:A6:87:9D:E2:49:CF:25:A5:27:14:EE:A0:45:CE:E3:32:21:DC:8D:A5:AE:78:36:EF:5A:9

1:D6:7E:D9:F4:04:C5:A9:9A:38:F7:D4:C6:50:B2:4C:96:1C:AE:69:23:19:7C:45:87:07:37:4C:2C:07:25:87:6C:93:D0:B6:D0:5D:55:FC:29:A0:48:6A:75:CF:12:6C:41

:AE:90:BD:E7:89:C5:C4:8D:81:78:3D:DD:0B:29:61:92:55:0E:5A:8F:44:8F:44:CE:07:D8:11:95:7F:03:33:DD:86:E0:9A:69:42:AD:C9:67:44:91:FF:B2:02:ED:1A:16:

9C:B5:CC:03:92:3B:1A:17:52:D5:32:56:BF:52:D1:7C:8F:96:43:18:6E:43:22:55:32:01:4D:44:AA:52:13:6A:BB:B6:1B:DD:8D:76:D3:C6:C2:D0:D9:E0:9E:B8:4C:DD:

0A:8D:5C:5E:20:02:79:20:26:84:7F:35:B7:EF:E0:98:D1:FC:37:D4:1B:B8:4C:07:64:00:E8:18:DC:63:98:85:56:F3:D0:F7:E4:EF:F1:C1:0F:B3:F2:86:48:73:36:A5:5D

:AC:A9:A9:DE:F9:62:44:D0:C8:8D:F1:03:5F:3E:03:08:C8:0C:92:00:CF:72:55:02:03:01:00:01",

"issuedByRootCertificate": false,

"privatekeyAvaliable": true,

"resourceId": "5f4e5c2e70040d33314f0e9d"

}

],

"totalRecords": 1,

"obtainedRecords": 1,

"obtainedRecordRange": {

"start": 1,

"end": 1

}

},

"message": "Matching results found for the given input.",

"appStatusCode": null,

"tags": null

},

"message": null,

"appStatusCode": null,

"tags": {},

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Add Certificate Attributes

The add certificates attributes API initiates the addition of various attributes like name, label, etc. to the certificate.

Before you begin

- The user has the ACF permission to add certificate attributes.
- A certificate attribute with the specified name and label combination should not already exist.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/attribute
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attribute?gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. It consists of an array of attributes listed below. The array cannot be empty; a minimum of one entry must be present. **Type**: Payload

Payload

Payload

Name	Description
name	(Mandatory) The name of the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
label	(Mandatory) The label to be shown on the UI for the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
value	(Optional) Default value for the attribute. **Type**: String
mandatory	(Optional) Indicates whether the attribute is mandatory or optional. **Type**: Boolean
helpInfo	(Optional) Help information about the field. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response attributes.
successfullFields response	List of fields that have been added successfully. **Type**: Array of CertificateGenericField
failedFields response	List of fields that have not been added successfully. **Type**: Array of CertificateGenericField
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 Accepted	NA	The response messages are as follows: • If all fields are added - **Certificate attribute added successfully** • If the addition of some fields have failed - **Certificate attribute added successfully. Failed fields are [<<failed field names>>]** • If the addition of all fields failed - **Certificate attribute addition failed.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation Validate the inputs based on the following failure reasons: • Name or label are not provided for the failed field. • Value provided for the name or label does not meet the expected pattern. • Attributes with the provided name already exists.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - payload. **Remediation**: Payload array cannot be empty. At least one attribute must be provided.
400 Bad Request	avx-common-028	Invalid / Incorrect payload. **Remediation**: Check and ensure that the values provided for all the fields in the payload are accurate.

Sample Request/Response

Request Payload

```
[
 {
 "name": "externalemail",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"label": "External_Email",
"value": "test@test.com",
"mandatory": true,
"helpInfo":"The external email id"
},
{
"name": "priority",
"label": "priority",
"value": "1",
"mandatory": false
}
]
```


Response


```
{
"response": {
"failedFields": [],
"successfullFields": [
{
"id": "externalemailcustomAttributecustomAttribute",
"type": "text",
"value": "test@test.com",
"values": null,
"label": "External_Email",
"searchKey": "externalemail",
"errorCode": null,
"mandatory": true,
"validation": null,
"divClasses": null,
"classNames": null,
"category": "certAttributes",
"certificateAuthority": null,
"regexValue": null,
"helpInfo": "The external email id",
"name": "externalemail",
"mandatoryFor": null,
"_id": "externalemail"
},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
"id": "prioritycustomAttributecustomAttribute",
"type": "text",
"value": "1",
"values": null,
"label": "priority",
"searchKey": "priority",
"errorCode": null,
"mandatory": false,
"validation": null,
"divClasses": null,
"classNames": null,
"category": "certAttributes",
"certificateAuthority": null,
"regexValue": null,
"helpInfo": null,
"name": "priority",
"mandatoryFor": null,
"_id": "priority"
}
]
},
"message": "Certificate attribute added successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


What's next?

Get Certificate Attributes

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Add Multiple Certificate Attributes

This API will let you add multiple certificates attributes for a certificate based on the certificate UUID or the resource ID.

Before you begin

- The user has the ACF permission to add certificate attributes.
- Certificate attributes with the specified name and label combination should not already exist.

Request Structure

Endpoint:	/certificate/attributeValues
Type:	POST

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attributeValues?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. It consists of an array of attributes listed below. The array cannot be empty; a minimum of one entry must be present. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
certAttributes	(Mandatory) A nested JSON that contains the key-value pairs for the attributes to be added for the certificate **Type**: JSON **Constraint**: Attribute name and value should not contain invalid (HTML and XML) characters.
resourceId	(Mandatory if **certificateUuid** is not provided) Unique identifier associated with the certificate **Type**: String **Note:** It is recommended to use the resource ID since the use of certificate UUID will be deprecated in the future.
certificateUuid	(Mandatory if **resourceId** is not provided) Unique Identifier assigned to the certificate **Type**: String **Note:** It is recommended to use the resource ID since the use of certificate UUID will be deprecated in the future.
action	(Mandatory) Action to be performed by executing this API **Type**: String **Possible value**: add
category	(Optional) Certificate category **Type**: String **Constraints**: Parameter value cannot be **CA**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Success Response

200 OK Response with message	Certificate attributes saved to certificate successfully
Response content-Type:	application/json

Response Parameters

Name	Description
response	Response for the add request
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response

Status Codes

HTTP Code	appStatusCode	Message and Possible remediation
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Mandatory field is missing or has invalid value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Message and Possible remediation
		Possible remediation: Ensure that the mandatory field specified in the error message is present in the payload and is assigned an accepted value.
400 Bad Request	AVX-VLDN-001	Mandatory field is missing or has invalid value. **Possible remediation**: Ensure that the mandatory field specified in the error message is present in the payload and is assigned an accepted value.
404 Not Found	CERT-INV-0021	Certificate(s) for the given resource ID/certificate UUID are unavailable in the certificate inventory. **Possible remediation**: Ensure that there is a corresponding certifcate for the given resource ID/certificate UUID.
404 Not Found	AVX-VLDN-001	Either the certificate UUID or resource ID should be present in the request. **Possible remediation**: Ensure that a valid resource ID/certificate UUID is present in the request.
403 Forbidden	CERT-ACF-0058	User does not have relevant permission to perform this action. **Possible remediation**: Ensure that the user has the required ACF

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Message and Possible remediation
		permissions to export certificates for a given module.
403 Forbidden	ACF_GW_005	User does not have access to the targeted API **Possible remediation**: Ensure that the user has the required ACF permissions to export certificates for a given module.

Sample Request/Response

Sample Request


```
{
   "certAttributes": {
      "test2": "CERT+_ACCTest2",
      "test3": "CERT+_ACCTest3",
      "test4": "CERT+_ACCTest4",
      "test5": "CERT+_ACCTest4",
      "expiryNotification":"expiryNotification"
   },
   "category":"server",
   "action": "add",
   "certificateUuid": "08bd683de4fe75c3a611032201ea212fbe72f3f2",
   "resourceId": "66192b925c61db504033113e1"
}
```


Sample Response


```
{
   "response": null,
   "message": "Certificate attributes saved to certificate successfully.",
   "appStatusCode": null,
   "tags": null,
   "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Update Certificate Attributes

The update certificates attributes API initiates a request to update the existing certificate attributes.

Before you begin

- The user should have the ACF permission to modify certificate attributes.
- The certificate attribute with the specified name and label combination should already exist.

Request Structure

Endpoint:	/certificate/attribute

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attribute?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. The array cannot be empty; a minimum of one entry must be present.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Type: Payload

Payload

Payload

Name	Description
name	(Mandatory) The name of the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
label	(Mandatory) The label to be shown on the UI for the custom attribute. **Type**: String **Constraint**: Must not start with special characters. No special characters except -, _ are allowed.
value	(Optional) Default value for the attribute. **Type**: String
mandatory	(Optional) Indicates whether the attribute is mandatory or optional. **Type**: Boolean
helpInfo	(Optional) Help information about the field. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

updateCertAttrResponse

Name	Description
updatedGenericFields response	List of fields updated **Type**: Array of CertificateGenericField
failedGenericFields response	List of fields that could not be updated successfully **Type**: Array of CertificateGenericField
addedGenericFields response	List of new fields added **Type**: Array of CertificateGenericField

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate attribute updated successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - payload. **Remediation**: Payload array cannot be empty. At least one attribute must be provided.
400 Bad Request	avx-common-028	Invalid / Incorrect payload. **Remediation**: Check and ensure that the values provided for all the fields in the payload are accurate.

Sample Request/Response

Request Payload


```
[
{
"name": "approver",
"label": "approver",
"value": "cert approver",
"mandatory": true
}
]
```


Response


```
{
"response": {
"updatedGenericFields": [
{
"id": "approvercustomAttribute",
"type": "text",
"value": "cert approver",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"values": null,
"label": "approver",
"searchKey": "approver",
"errorCode": null,
"mandatory": true,
"validation": null,
"divClasses": null,
"classNames": null,
"category": "certAttributes",
"certificateAuthority": null,
"regexValue": null,
"helpInfo": null,
"name": "approver",
"mandatoryFor": null,
"_id": "approver"
}
],
"failedGenericFields": [],
"addedGenericFields": []
},
"message": "Certificate attribute updated successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


What's next?

Delete Certificate Attributes

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Get Certificate Attributes

The get certificates attributes API fetches all the certificate attributes.

Before you begin

- The user should have the required ACF permission to view the certificate attributes.

Request Structure

Endpoint:	/certificate/attribute
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attribute?gwsource=external` To understand the elements of the sample URL, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: Array of CertificateGenericField
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 Accepted	NA	Certificate attributes fetched successfully. OR No certificate attributes available.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
406 Not Acceptable	CERT-GFLD-0005	Certificate attributes fetch failed. ${ERROR_MSG} In case of any unexpected error message

Sample Request/Response

Request Payload

No payload for GET request

Response

```
{
 "response": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
"id": "approvercustomAttributecustomAttribute",
"type": "text",
"value": "cert approver",
"values": null,
"label": "approver",
"searchKey": "approver",
"errorCode": null,
"mandatory": true,
"validation": null,
"divClasses": null,
"classNames": null,
"category": "certAttributes",
"certificateAuthority": null,
"regexValue": null,
"helpInfo": null,
"name": "approver",
"mandatoryFor": null,
"_id": "approver"
}
],
"message": "Certificate attributes fetched successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


What's next?

Update Certificate Attributes

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Delete Certificate Attributes

The delete certificates attributes API initiates a request to delete the existing certificate attributes.

Before you begin

- The user should have the ACF permission to delete certificate attributes.
- The certificate attribute with the specified name and label combination should already exist.

Request Structure

Endpoint:	/certificate/attribute
Type:	DELETE
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attribute?gwsource=external`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To understand the elements of the sample URL, click here.
Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
name *Query*	(Mandatory) Name of the certificate attribute that has to be deleted. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Message indicating whether the field has been successfully deleted or not. **Message**: *Deleted Successfully - [approver1]. Failed to delete - []*
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Certificate attribute deleted successfully.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the value provided for the name query parameter is accurate.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the name query parameter is available in the request.

Sample Request/Response

Request Payload

No payload for DELETE request.

Response


```
{
 "response": "Deleted Successfully - [approver2]. Failed to delete - []",
 "message": "Certificate attribute deleted successfully",
 "appStatusCode": null,
 "tags": {},
 "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Delete Multiple Certificate Attributes

This API will let you delete multiple certificate attributes present for a certificate based on the certificate UUID or the resource ID.

Before you begin

- The user should have the ACF permission to modify certificate attributes.
- The certificate attributes with the specified name and label combination should already exist.

Request Structure

Endpoint:	/certificate/attributeValues
Type:	DELETE
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attributeValues?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Possible values**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. It consists of an array of attributes listed below. The array cannot be empty; a minimum of one entry must be present. **Type**: Payload

Payload

Payload

Name	Description
certAttributes	(Mandatory) List of attributes to be deleted **Type**: JSON

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: • Each attribute in this list should be present in the AppViewX certificate attribute settings. • Attribute name and value should not contain invalid (HTML and XML) characters.
resourceId	(Mandatory if **certificateUuid** is not provided) Unique identifier associated with the certificate **Type**: String **Note:** It is recommended to use the resource ID since the use of certificate UUID will be deprecated in the future.
certificateUuid	(Mandatory if **resourceId** is not provided) Unique Identifier assigned to the certificate **Type**: String **Note:** It is recommended to use the resource ID since the use of certificate UUID will be deprecated in the future.
category	(Optional) Certificate category **Type**: String **Constraints**: Parameter value cannot be **CA**.

Response Structure

Success Response

200 OK Response with message	Certificate attributes saved to certificate successfully

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Success Response (continued)

Response content-Type:	application/json

Response Parameters

Name	Description
response	Contains the response attributes for the delete request
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response

Status Codes

HTTP Code	appStatusCode	Message and Possible remediation
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Mandatory field is missing or has invalid value. **Possible remediation**: Ensure that the mandatory field specified in the error message is present in the payload and is assigned an accepted value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Message and Possible remediation
400 Bad Request	AVX-VLDN-001	Mandatory field is missing or has invalid value. **Possible remediation**: Ensure that the mandatory field specified in the error message is present in the payload and is assigned an accepted value.
404 Not Found	CERT-INV-0021	Certificate(s) for the given resource ID/certificate UUID are unavailable in the certificate inventory. **Possible remediation**: Ensure that there is a corresponding certifcate for the given resource ID/certificate UUID.
404 Not Found	AVX-VLDN-001	Either the certificate UUID or resource ID should be present in the request. **Possible remediation**: Ensure that a valid resource ID/certificate UUID is present in the request.
403 Forbidden	CERT-ACF-0058	User does not have relevant permission to perform this action. **Possible remediation**: Ensure that the user has the required ACF permissions to export certificates for a given module.
403 Forbidden	ACF_GW_005	User does not have access to the targeted API **Possible remediation**: Ensure that the user has the required ACF permissions to export certificates for a given module.
417 Expectation Failed	CERT-FV-001	Invalid query param found for <Query Param>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Message and Possible remediation
		Possible remediation: Ensure that the mandatory field specified in the error message is present in the query and is assigned an accepted value.

Sample Request/Response

Sample Request

Delete request will not have any payload. It will have query params.

```
/certificate/attributeValues?ttl=300&gwkey=f000ca01&gwsource=api&resourceId=6618c4573d3dd048316c4593&certificateUuid=08bd683de4fe75c3a611032201ea212fbe72f3f2&certattributes=test1,test2&category=server
```

Sample Response

```
{
    "response": null,
    "message": "Certificate attributes  are deleted successfully and certificate attributes test2, test1 are not attached with certificate",
    "appStatusCode": null,
    "tags": {},
    "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Bulk Add/Update Certificate Attributes

This API allows you to add or update one or more certificate attributes for one or multiple certificates in a single API request.

Before you Begin

- Ensure that the user has the required permissions to add and update certificate attributes.

Request Structure

Endpoint:	/certificate/attributeValues
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/attributeValues?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (for example, external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the PUT request. **Type**: Payload

Payload

Payload

Name	Description
resourceIds	(Mandatory if `resourceIdList` is not specified) Resource ID of the certificate for which the attributes in the payload have to be added and/or updated The `resourceIds` parameter is used when one or more attributes have to be added an/or updated for a single certificate. Certificate resources IDs can be retrieved using the /certificate/search API.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Note:** It is recommended that `resourceIdList` is used instead of `resourceIds` because `resourceIds` will be deprecated soon.
resourceIdList	(Mandatory if `resourceIds` is not specified) Comma-separated list of resource IDs of all certificates for which the attributes in the payload have to be added and/or updated The `resourceIdList` parameter is used when one or more attributes have to be added and/or updated for multiple certificates. **Type**: Array
attributeValues	(Mandatory) A nested JSON containing the key-value attribute pairs to added and/or updated for the specified certificate(s) The key represents the attribute name and the value is the value being assigned to the specified attribute. **Type**: JSON **Constraints**: • The value of the date attribute should be in the GMT time zone. • The certificate attribute name and value should be assigned valid values as defined in the product.

Response Structure

Success Response

200 OK Response with the message: Certificate attribute updated successfully.

Response content-type: application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters

Name	Description
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

Status Codes

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason: Invalid credentials **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field missing or invalid value **Remediation**: Ensure that the missing mandatory field, as specified in the error response, is included in the payload and is assigned a valid value.
400 Bad Request	RESOURCE_ID_EMPTY	Either both the `resourceIds`and `resourceIdList` parameters are not

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		specified or do not have a value assigned. **Remediation**: Ensure that either one of the parameters, `resourceIds` and `resourceIdList`, is specified and is not empty.
400 Bad Request	CertAttributeBulkError-020	Invalid date format **Remediation**: Ensure that the value for the date attribute is a valid format, such as **MM/dd/yyyy**, **yyyy-MM-dd**, **dd-MM-yyyy** or one of the ISO 8601 formats (like **MM/dd/yyyy HH:mm** or **MM/dd/yyyy HH:mm:ss**) .
404 Bad Request	INVALID_REQUEST	Both `resourceIds` and `resourceIdList` are specified in the payload. **Remediation**: Only of the two parameters, `resourceIds` and `resourceIdList`, must be specified at a time.
403 Forbidden	CERT-ACF-0058	User does not have the required permissions for performing this action. **Remediation**: Ensure that the user has all the requisite permissions for

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		adding/updating certificate attributes.
403 Forbidden	ACF-GW-005	User does not have access to the target API. **Remediation**: Ensure that the user has the requisite ACF permissions to add and update certificate attributes.
404 Not Found	RESOURCE_ID_NOT_AVAILABLE_OR_PERMISSION_DENIED	• One or more of the resource IDs specified are unavailable. • User does not have the permission to add and update the certificate attributes for certificates with the specified resource IDs. **Remediation**: Ensure that all resource IDs specified in the payload are valid (have a corresponding certificate) and that the user has all the requisite permissions to add and update the attributes.
417 Expectation Failed	CERT_ATTRIBUTE_NOT_AVAILABLE	The specified certificate attribute is not defined in the AppViewX product. **Remediation**: Ensure that the certificate attribute

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		name is already defined in the AppViewX product.
417 Expectation Failed	CERT_ATTRIBUTE_NOT_AVAILABLE	Certificate attribute value is invalid. **Remediation**: Ensure that the new certificate attribute value provided is a valid value for that attribute.

Sample Request/Response

Sample Request


```
{
 "attributeValues": {
  "test": "testValue123",
  "dropdown": "test",
  "Date": "1751278741000",
  "expiryNotification": "false"
 },
 "resourceIdList: [
  "67bc2ca76a105e1a05691c1c",
  "67bc2ca76a105e1a05691c2c",
  "67bc2ca76a105e1a05691c3c"
 ]
}
```


Sample Response


```
{
 "response": null,
 "message": "Certificate attribute(s) value updated successfully",
 "appStatusCode": null,
 "tags": { },
 "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Fetch List of Server Devices

This API will fetch the list of server devices onboarded in AppViewX based on the status and vendor specified.

Before You Begin

Before attempting to fetch this list, ensure the following:

- Devices should be added in the server device inventory.
- Users should have permission of **Platform** > **Asset Management** > **Device Inventory** > **Servers**.
- Users should have read permission to the added devices.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificates/devices/servers
Type:	GET
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificates/devices/servers?vendor=Apache&status=Managed&page=3&limit=4&gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId or **auth token** *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password **Type**: String
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String **Possible values**: application/json
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
	Type: Payload

Payload

Payload

Name	Description
vendor	(Optional) Name of the server device vendor **Type**: Sting **Possible values**: For the full list of supported server device vendors, click here.
page	(Optional) Starting page in the inventory to being the search **Type**: Integer **Default value**: 1 **Constraints**: Only positive integer values allowed
limit	(Optional) Maximum number of records to be fetched (beginning from the starting **page**) **Type**: Integer **Default value**: 100 **Constraints**: • Only positive integer values allowed • Maximum limit value: 100
Status	(Optional) Device status value to be included in the search query **Type**: String **Constraints**: The status should be a valid value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values: • Unresolved • Failed • InProgress • Managed • Queued

Response Structure

Success Response

200 OK response with the list of devices from the device inventory

Response content-type: application/json

Response Parameters

Name	Description
response	Contains the response attributes for the fetch request **Type**: response
message	Success message of the action or failure description (in case of error) **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

response

Name	Description
credentialType	Authentication mechanism used by AppViewX to access and managed privileged accounts **Type**: String **Possible values**: Manual entry, Credential list-AppViewX, SSH, etc.
hostName	Unique name assigned to identify the device within the network **Type**: String
operatingSystemType	Operating system installed on the device **Type**: String
fqdn	IP address/Fully Qualified Domain Name of the device within the network **Type**: String
dataCenter	Data center where the device is hosted **Type**: String
port	Communication port of the device **Type**: Integer
vendor	Name of the device vendor **Type**: String
name	Device name used in AppViewX **Type**: String
certSyncStatus	Certificate parsing status **Type**: String
version	Device version number

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

response (continued)

Name	Description
	Type: String
status	Device status in AppViewX **Type**: String **Possible values**: Managed, Failed, Unresolved, etc.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
403 Forbidden	CERT-ACF-0058	User does not have access to the targeted API **Possible remediation**: Ensure that the user has the required ACF permissions to export certificates for a given module.
407 Proxy Authentication Required	AVX_GW_011	Session validation failed; reason: Session information is missing **Possible remediation**: Provide correct authentication parameters.
400 Bad Request	MISC_VAL_005	Invalid query param for 'xxx' **Possible remediation**: Ensure that the field mentioned in the error message is assigned an accepted value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Sample Request

```
GET /avxapi/certificates/devices/servers?vendor=Apache&status=Managed&page=3&limit=4&gwsource=external
```

Sample Response


```
{
  "response": {
    "data": [
      {
        "credentialType": "Manual Entry",
        "hostName": null,
        "operatingSystemType": null,
        "fqdn": "pe-adc-apvx-n3.lab.appviewx.net",
        "dataCenter": "absecon",
        "port": 22,
        "vendor": "Apache",
        "name": "pe-adc-apvx-n3.lab.appviewx.net",
        "certSyncStatus": "Completed",
        "version": "",
        "status": "Managed"
      },
      {
        "credentialType": "Manual Entry",
        "hostName": null,
        "operatingSystemType": null,
        "fqdn": "pm-saas-node18.lab.appviewx.net",
        "dataCenter": null,
        "port": 22,
        "vendor": "Apache",
        "name": "pm-saas-node18.lab.appviewx.net",
        "certSyncStatus": "Completed",
        "version": "",
        "status": "Managed"
      }
    ],
    "iTotalDisplayRecords": 2
  },
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "message": null,
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Download a Certificate

The download certificate API can download a certificate in PEM format. If desired, the user can also request the certificate to be downloaded along with the key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

- The user should have the ACF permission to download the certificate within the specified certificate's category.
- A certificate with the resource ID specified for deletion should already exist.
- The group associated with the certificate should at least have the R permission.

Request Structure

Endpoint:	/certificate/download
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/download?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource	(Mandatory) Source from which the request is triggered. (E.g. external)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
resourceId	(Mandatory) Unique Id of the certificate to be downloaded.
Query	**Type**: String
keyRequired	(Optional) Indicates whether the private key needs to be downloaded.
Query	**Type**: Boolean
isCACertificate	(Optional) Indicates whether the certificate being downloaded is a CA certificate.
Query	**Type**: Boolean

Response Structure

Status Code:	200 OK
Error Response:	The error response will have the parameters described below.
Headers	
Content-Type:	application/octet-stream

Error response parameters

Name	Description
message	Failure description. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	The attachment of the **.pem** type certificate.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Ensure that the value provided for resourceId parameter refers to the id of an existing certificate.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - resourceId. **Remediation**: Ensure that the resourceId parameter is available in query parameter.
417 Expectation Failed	NOT_A_VALID_CERT	Invalid certificate. **Remediation**: Certificates that have not yet been issued cannot be downloaded. Ensure that the resourceId refers to the certificate that has been issued.
417 Expectation Failed	CERT-KEY-0006	Private key access is restricted in <<Default>> policy. **Remediation**: Retry downloading the certificate after enabling the flag **Enable Access to Private Key** in the Certificate Policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Response

The downloaded file is a **pem** file and the content of the downloaded file is as mentioned in the example below:

```
-----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
b24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
b3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAlthtOgQ3pOsqTQNroBvo3bSMgHFzZM
9O6II8c+6zf1tRn4SWiw3te5djgdYZ6k/oI2peVKVuRF4fn9tBb6dNqcmzU5L/qw
IFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
VOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
93FcXmn/6pUCyziKrlA4b9v7LWIbxcceVOF34GfID5yHI9Y/QCB/IIDEgEw+OyQm
jgSubJrIqg0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMC
AYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
A4IBAQCY8jdaQZChGsV2USggNiMOruYou6r4lK5IpDB/G/wkjUu0yKGX9rbxenDI
U5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
N+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
o/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
rqXRfboQnoZsG4q5WTP468SQvvG5
-----END CERTIFICATE-----
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Download a Certificate by Format

The download certificate by format API initiates a request to download a certificate in the requested format. The user can request the private key to be downloaded in the specified format as well. The key can be requested with or without encryption. Additionally, the user can specify whether the complete certificate chain needs to be downloaded.

Before you begin

- The user should have the ACF permission to download the certificate within the specified certificate's category.
- A certificate with the resource ID (or the common name and serial number combination) specified for deletion should already exist.
- The group associated with the certificate should at least have the R permission.

Request Structure

Endpoint:	/certificate/download/format
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/download/format?gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	The payload contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
format	(Mandatory) The format of the certificate to be downloaded. **Type**: String **Constraint**: The possible certificate formats are - **CRT**, **CERT**, **CER**, **PEM**, **DER**, **DERCER**, **P7B**, **P7C**, **PK8**, **P12**, **PFX**, and **JKS**.
password	(Optional) Password for the certificate. It is applicable for the following certificate formats: **P12**, **PFX**, **JKS**, and **PK8**. (Mandatory) Password is mandatory for the following certificate formats: **P12**, **PFX**, and **JKS**. **Type**: String
commonName	(Mandatory if resourceId is not provided) Common name of the certificate. **Type**: String
serialNumber	(Mandatory) Serial number of the certificate to be downloaded **Type**: String
resourceId	(Mandatory if commonName and serialNumber are not provided) Certificate ID to download the certificate content **Type**: String
isChainRequired	(Optional) Indicates whether to download the complete certificate chain or only the end certificate. **Type**: Boolean
isKeyEncryptionRequired	(Optional) Indicates whether the private key should be encrypted using a password.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Boolean **Constraint**: This is applicable for PK8 format. If the value is **true**, • Ensure that the certificate policy allows private key access. • The password must be provided in the request payload.

Response Structure

Status Code:	200 OK
Error Response:	The error response will have the parameters described below.
Headers	
Content-Type:	application/octet-stream

Error response parameters

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	The attachment of the **.pem** type certificate.
404 Not Found	NO_RECORDS_FOUND	No matching records found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the value provided for commonName and serialNumber pertain to that of a valid existing certificate.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field>> **Remediation**: Ensure that the **<<field>>** is available in the request payload.
400 Bad Request	INVALID_FORMAT	Invalid format specified. **Remediation**: Ensure that a valid value is provided in the format field of the request.
417 Expectation Failed	NOT_A_VALID_CERT	Invalid certificate. **Remediation**: Certificates that have not yet been issued cannot be downloaded. Ensure that the resourceId refers to the certificate that has been issued.
417 Expectation Failed	CERT-KEY-0006	Private key access is restricted in <<Default>> policy. **Remediation**: Retry downloading the certificate after enabling the flag

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Enable Access to Private Key in the Certificate Policy.
417 Expectation Failed	CERT-HLST-0007	Failed to download as the given extension is not supported. **Remediation**: Ensure that a valid value is provided for the format field in the request.
417 Expectation Failed	PASSWORD_FORMAT_WRONG	Password must have at least eight characters and contain at least one lowercase letter, one uppercase letter, one numeric digit, and one special character. **Remediation**: Password provided in the request payload must have at least eight characters and contain at least one lowercase letter, one uppercase letter, one numeric digit, and one special character.

Sample Request/Response

Request Payload

```
{
"commonName" : "testcert7a.appviewx.com",
"serialNumber" : "07:2B:84:01:27:5A:77:63:38:C8:72:09:BE:CD:1F:D9:78:BA:BD",
"format" : "P12",
"password":"Password@123",
"isChainRequired":true,
"isKeyEncryptionRequired":false
}
```

Response

File is downloaded in the requested format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Download Private Key of a Certificate

The download private key of a certificate API downloads the private key of a certificate in the password protected PEM format.

Before you begin

- The user should have the ACF permission to download the private key within the specified certificate’s category.
- A certificate with the UUID specified for deletion should already exist.
- Private key access should be enabled under the certificate policy of the associated certificate group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/privatekey/download
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/privatekey/download?gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
uuId	(Mandatory) Universally Unique Identifier (UUID) of the certificate of which the private key is to be downloaded **Type**: String
password	(Optional) Password for encrypting the private key in the response. **Type**: String

Response Structure

Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
privateKeyPemEncoded	Private key of certificate in password encrypted pem. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
success	**True** if download is successful and **False** if error in downloading. **Type**: Boolean
tags	Additional information in case of failure response.

response

Name	Description
status	Status of the download request **Type**: String
zipFileName	Name of the zipped file that contains the downloaded private key **Type**: String
certContents	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
privateKeyPemEncoded	Private key of certificate in password encrypted pem. **Type**: String
success	**True** if download is successful and **False** if error in downloading. **Type**: Boolean
log	Additional information in case of failure response

Status Codes

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-GEN-0015	Field cannot be null/empty. **Remediation**: Ensure the mandatory fields have valid value in the request. It should not be null or empty.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-KEY-0006	Private key access is restricted in <policy> policy. **Remediation**: Enable private key access in the mentioned policy.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid. **Remediation**: Ensure all the mandatory fields have valid value in the request.
500 Internal Server Error	CERT-GEN-0027	Certificate private key download failed.

Sample Request/Response

Request Payload


```
{
"uuId": "60b8d6c4e5c7a920d4f4f1f4",
"password": "testPassword123"
}
```


Success Response


```
{
 "response": {
 "status": "Success",
 "zipFileName": null,
 "certContents": null,
 "privateKeyPemEncoded": "-----BEGIN ENCRYPTED PRIVATE
 KEY-----\nMIIE9jAoBgoqhkiG9w0BDAEDMBoEFEC4EngLMd1kbUJjHxgNyvApBAMFAgIIAASC\nBMhv4AkofevTbEa0BZ3HLOI/WIHelmYmHtwC26SDI1JGJWK
UN1O0W52rIn30mjZG\niUxiu7F3ozQgrKBCHuM+lKxx4zYbmgukyodJtbzJ4EohmapiZQHJSf4DiJiHHa8X\nZ/r
+sfNoRunhy3r/0SS0lNZqQvnM5dqSATkHTtrcD82NsKIx4GScFfG5yKhoAsS6\nEJQag7THPAbwaRPml54UZBsFnjmkG638utC511EWdbD0Z12L4zxhzPNxgnYF
NQEg\n12552kjj5jGNZgojxZ52BpWe0ZfDkH+bvt7LC9M62n4d5vrivlfBd6R7ZMjDAD0M\nn2vtltgoKe9Nbxq/5oraGJt+8ql/sWlGWehx/L8Ue/weCzXtmectQd69M4id
K7QQ\nAwOh/cdosut6uQUGzIrH3n59INWbkJ0HzlunJjLcvJzrhr191SYmMU0HNPjaVptD\n
+UErWYqs4y1XEwOn1jrNQ8cBA0VvkwhAu1juWc0hoY9s6tv573dnljrNAtiVOtw4\nl3CsQlNMAXSHizpaM6pKXh8mCHfgZqzDmbmDTTDc9A37ekgnDfSRCEgzR
KQl4bJT\noXYRJFTyjGqT4HdC9pKaj3B+IHfWae5iWOB5kCdaE9qCc9NjN8WzPed3U3ltNNzC\neW3mYihP+
+XCB9uNHyLZ9jCXh42RCCW/omVlgZR9VBvhrq3tmk8MCYp+cFdo2KsH\nlC+MAVL6NPI4jcGBNt2JUMG5coPXttF2OsHqucH95WqUDUBF5+ZmpvJSuCFb8
SEc\nvAH35lwJnanZs4hPIlgywkRcIdu+Mv
+lseOqFQvRypeRKPLGlWqZQZ83J5P2ENhv\nhQLv9hrYLKzpo4oMk4GTFeLNvYnayAa5sqAOACoI8QZRmjUPVffG3KEQ6F3vOTdX\n1BrpeSH6rbolqEUTcBpc
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

agf+1XdoZ4f3h76K0yVH1KVE8Gz2uQvWqm33UThVU2ra\n0kWLxO2tz3tN0m21MLQhU4bWDMT5Yz5GdsLLQQgkiIzZ7vwfnYT6xtTPTJLre0X+
\n927vNJnhVgtdydutSIMf+m
+tH3knZ35K8MCBH7lLV+Ov0dj4DSbD/44eMuBOP7KW\n8u4FK0Mys4EeBc2nH9tQ/HTSDCRJGj8sycRHZGGCRRAuFtIBXy0F9lnbaoTCNnIS\ngeW/ZjuSBHH0
csNxvJZS3rr62Pnl14lOueM5cklLa02LqON/gdRZwXQm7i0sOTEC\nvhX4Y3RgJ8+IZYx3MyeNKuUBFOuyRcl3my/C6K9okMyQhAgXr16YR/v/ioKihX8/\nRH0RC9
OrSy6ad0lLRhye9/giEJ2JBfKq8QwwRUO1peD7lrzsde6gD8c9XRmbshgu\ndU00dmL0a26H/h
+/T9UnS5D1KJUROHXeCX2ywakw/k1hR9xfiQsYJ6FVXGC38POW\nVnOK4gmRnGQPfDsqZJ32bm+cyqQ2nmXYHxGQO1S0k+U5JlmPk9EruaWal2rud8wO\nd
AcT/ZUxaBXXjwRnOAr142Hh939KuMcb7IK7as0Ku2xoBxLSGFIkaQXCnLVavs1C\nGNs0ZrN9rDwua7e7VTug08oI0H0Fvqt5cgQAaFTDjM6Usy7AoKJVoP4jl4Us
W78m\nTRAnJLIfDxCBX5b315bMMg5uTpZRDcIybY0=\n-----END ENCRYPTED PRIVATE KEY-----\n",
"success": true,
"log": false
},
"message": "private key downloaded successfully",
"appStatusCode": null,
"tags": {},
"headers": null
}

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Common Response Objects

This page contains fields that are used in APIs for add, update, and get certificate attributes. These fields are grouped together here because they are common to these APIs.

Parameters for CertificateGenericField

Name	Description
_id	Unique identifier for the attribute. **Type**: String
name	Name of the attribute. **Type**: String
type	Type of the attribute. **Type**: String
value	Default value for the attribute. **Type**: String
label	Label to be shown in the UI for the custom attribute. **Type**: String
searchKey	Keyword for searching the certificate based on the attribute. **Type**: String
mandatory	Indicates whether the attribute is mandatory or optional. **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters for CertificateGenericField (continued)

Name	Description
category	The category of the attribute will always be "certAttributes" for certificate attributes. **Type**: String
helpInfo	Help information about the field. **Type**: String

Push and Bind Certificate to a Firewall Profile

The push and bind certificate to a firewall profile API uploads the certificate and its private keys to the firewall profile and links them to the server profiles. Refer to After you are done section to Approve and Implement the request.

Before you Begin

Ensure the following before attempting to push and bind certificate to a firewall profile through AppViewX:

- Firewall devices must be configured in AppViewX.
- The devices should be in the Managed state.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String
selectedProfiles	(Mandatory) Firewall profile id. **Type**: String **Constraint**: If the profile connector is specified then certificate is **pushed** and **bound** to the profile, but if a default connector is specified then the certificate is only **pushed**.
certificateDetails	(Mandatory) Certificate details for the Firewall devices. **Type**: Any of the following type (as per the firewall device) - Refer the Fortinet certificate details OR PaloAlto certificate details tables respectively.
pushDetails	(Optional) Other push details **Type**: pushDetails

Fortinet certificate details

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: Value should be **PEM-.pem**.
certificateName	(Mandatory) Certificate name i.e. the name in which the certificate is to be pushed to the firewall device. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fortinet certificate details (continued)

Name	Description
	Constraint: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . It should not be the same as intermediate file name and CA file name.
privateKeyPassword	(Optional) Password for the private key pushed to the firewall device. **Type**: String
pushRootAndIntermediateCertificates	(Mandatory) Indicates whether the Root and Intermediate certificate are to be pushed to the firewall device. **Type**: Boolean **Constraint**: The value is either true or false.
rootCertificateFileName	(Mandatory) Root certificate name i.e. the name in which the root certificate is to be pushed to the firewall device. **Type**: String **Constraint**: The root certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.
intermediateCertificateFileName	(Mandatory) Intermediate certificate name i.e. the name in which the intermediate certificate is to be pushed to the firewall device. **Type**: String (multiple values) **Constraint**: The intermediate certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >,

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fortinet certificate details (continued)

Name	Description
	(,), ;, . and should not be the same as certificate file name and CA file name.

PaloAlto certificate details

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: Value should be **PEM-.pem** or **PKCS12-.p12**.
certificateName	(Mandatory) Certificate name i.e. the name in which the certificate is to be pushed to the firewall device. **Type**: String **Constraint**: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . It should not be the same as intermediate file name and CA file name.
pushRootAndIntermediateCertificates	(Mandatory) Indicates whether the Root and Intermediate certificate are to be pushed to the firewall device. **Type**: Boolean **Constraint**: The value is either true or false.
rootCertificateFileName	(Mandatory) Root certificate name i.e. the name in which the root certificate is to be pushed to the firewall device. **Type**: String **Constraint**: The root certificate name should not start and end with special characters. No special characters except !,

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

PaloAlto certificate details (continued)

Name	Description
	@, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.
intermediateCertificateFileName	(Mandatory) Intermediate certificate name i.e. the name in which the intermediate certificate is to be pushed to the firewall device. **Type**: String (multiple values) **Constraint**: The intermediate certificate name should not start and end with special characters. No special characters except !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . and should not be the same as certificate file name and CA file name.

pushDetails

Name	Description
preValidationScriptPath	(Optional) Location of the pre push script. **Type**: String
postValidationScriptPath	(Optional) Location of the post push script. **Type**: String
overwrite	(Optional) Indicates whether the certificate needs to be overwritten if already available. **Type**: Boolean
pushAutomatically	(Optional) Indicates whether the certificate needs to be pushed automatically when renewed. **Type**: Boolean

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

response

Name	Description
requestId	Request ID for push action for the application connector. **Type**: String
connectorId	Application connector ID. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	The selectedProfiles parameter is already available in the specified certificate. **Remediation**: Provide a different value for the selectedProfiles field.
404 Not Found	NO_RECORDS_FOUND	No matching records found - certificate not found. **Remediation**: Provide a correct value for the field certificateId.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0016	Connector with profiles {} already exists. **Remediation**: A profile connector is already available for the selected certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Change the certificateId or delete the existing connector.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload


```
{
 "certificateDetails": {
 "certificateType": "PEM-.pem",
 "certificateName": "testfile",
 "pushRootAndIntermediateCertificates": true,
 "rootCertificateFileName": "testrootfile.pem",
 "intermediateCertificateFileName": [
 "testinterfilelevel1.pem"
 ]
 },
 "pushDetails": {
 "preValidationScriptPath": "",
 "postValidationScriptPath": "",
 "overwrite": false,
 "pushAutomatically": false
 },
 "certificateId": "5f5b1fac77534426423bab57",
 "selectedProfiles": [
 "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST"
 ]
 }
```


Response


```
{
 "response": [
 {
 "requestId": "3",
 "connectorId": "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST:@389ed6f96387e3002cc6ac0678c07ffe70459abf"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
}

],

"message": "1 connector(s) saved and push opertaion has been triggered.",

"appStatusCode": null,

"tags": {},

"headers": null

}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Rollback Certificate to Firewall Profile

The rollback certificate to a firewall profile API rolls back the certificate and its private keys to the firewall profile and links them to the server profiles. Refer to the After you are done section to Approve and Implement the request.

Before you begin

Ensure the following before attempting to rollback certificate to a firewall profile through AppViewX:

- Firewall devices must be configured in AppViewX.
- The devices should be in Managed state.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/rollback
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
autoApproval *Query*	Indicates whether the auto-approval is needed for the action. **Type**: String **Constraint**: Value of the parameter should be **yes**.
Payload *Body*	Contains all the parameters to be sent in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
applicationConnectorIds	(Mandatory) Application connector ID **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response attributes. **Type**: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

response

Name	Description
requestId	Request ID for rollback action for the application connector **Type**: String
connectorId	Application connector ID **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	App connector rollback action initiated for 1 connector(s).
202 Accepted	NA	Operation cannot be completed for one or more devices as the 'Resource' allocated to you does not have write permission.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that users have access to the device.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0012	Application connector ids cannot be empty. **Remediation**: Please provide value for the field applicationConnectorIds.
417 Expectation failed	ERR_APPLICATION_CONNECTOR_LIST_RETRIVAL	Unable to retrieve connector information. **Remediation**: Connector may not be available. Please

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_APP_CONNECTORS_NOT_FOUND	Application connector(s) not found. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_INITIALIZE_ROLLBACK_REQUEST	Unable to initialize rollback request.
417 Expectation Failed	ERR_ROLLBACK_INELIGIBLE	Push not triggered or succeeded or No existing data available for backup process **Remediation**: Push and bind certificate before rollback.
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

```
{
"applicationConnectorIds": [ "xx.xxx:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
}
```

Response

```
{
"response": [
{
"requestId": "386",
"connectorId": "panorama:@:@panorama:@panorama:@SSL/TLS
 Profile:@multiple_ssl_tls_service_profile_1:@cb162ef65e0ae8c4bdfd37b24d4d1bd7624be78d"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
}

],

"message": "App connector rollback action initiated for 1 connector(s).",

"appStatusCode": null,

"tags": {},

"headers": null

}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Get Available Server Profiles

The get available server profiles API fetches the available profile details for the particular server device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

Ensure the following before attempting to fetch available profiles for a particular server device through AppViewX:

- Server devices must be configured in AppViewX.
- The devices should be in Managed state.

Request Structure

Endpoint:	/certificate/profiles
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external&category=Server&vendor=<Vendor_Name>` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
category *Query*	(Mandatory) It specifies the device category. **Type**: String **Constraint**: Required if sessionId is not provided.
vendor *Query*	Vendor for the chosen device. For example, **Apache** is a vendor for the Server category. It is a mandatory field. **Type**: String
certificateUuid *Query*	Uuid of the certificate. **Type**: String
deviceName *Query*	Name of the device as per AppViewX Device Inventory. **Type**: String
inventory *Query*	Name of AppViewX inventory where the certificate is present.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the fetch profiles request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
objects	List of available device profile Ids.
response	**Type**: String
totalRecords	Total number of profiles fetched.
response	**Type**: Integer
obtainedRecords	Total number of profiles fetched.
response	**Type**: Integer
obtainedRecordRange	Range of record retrieved
response	**Type**: Object
start	Start index of the record range retrieved
response.obtainedRecordRange	**Type**: Integer
end	End index of the record range retrieved
response.obtainedRecordRange	**Type**: Integer
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	<<No. of profile Ids>> record(s) found

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	The mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Provide correct values for all the fields.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload

No payload for GET request

Response


```
{
"response":{
"objects":[
"ApacheLinux",
"ApacheLinux:@/etc/apache2:@xxx.xxx.xxx.xxx:@443:@/etc/apache2/sites-enabled/test.conf",
"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf",
"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-enabled/random-ssl.conf"
],
"totalRecords":4,
"obtainedRecords":4,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"obtainedRecordRange":{
"start":0,
"end":0
}
},
"message":"4 record(s) found",
"appStatusCode":null,
"tags":{

},
"headers":null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Push and Bind Certificate to a Server Profile

The push and bind certificate to a server profile API uploads the certificate and its private keys to the server device and links them to the server profiles. Refer to After you are done section to Approve and Implement the request.

Before you Begin

Ensure the following before attempting to push and bind certificate to a firewall profile through AppViewX:

- Server devices must be configured in AppViewX.
- The devices should be in Managed state.
- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username	(Mandatory) AppViewX login username.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String
selectedProfiles	(Mandatory) Server profile id.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraint**: If the profile connector is specified then certificate is **pushed** and **bound** to the profile, but if a default connector is specified then the certificate is only **pushed**.
certificateDetails	(Mandatory) Certificate details for the Firewall devices. **Type**: Any of the following type (as per the server device) - Refer the following: • Certificate details for IIS Server • Certificate details for Microsoft PC Server • Certificate details for Microsoft Server • Certificate details for Apache Linux Server • Certificate details for Tomcat Server • Certificate details for Weblogic Server • Certificate details for Websphere Server • Certificate details for IPlanet Server
pushDetails	(Optional) Other push details.
preValidationScriptPath pushDetails	(Optional) Location of the pre push script. **Type**: String
postValidationScriptPath pushDetails	(Optional) Location of the post push script. **Type**: String
overwrite pushDetails	(Optional) Indicates whether the certificate needs to be overwritten if already available. **Type**: Boolean **Constraint**: Enabled by default for IIS vendor.
pushAutomatically	(Optional) Indicates whether the certificate needs to be pushed automatically when renewed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
pushDetails	**Type**: Boolean

Certificate details for IIS Server

Name	Description
locationType	(Mandatory) Specifies whether the certificate should be uploaded to the certificate store or the centralized file system. **Type**: String **Constraints**: The allowed values are **Certificate store** or **File system**.
keyStoreLocation	(Mandatory) When the locationType "Certificate store" is chosen, the keyStoreLocation determines the sub-store under which the certificate should be uploaded. **Type**: String **Constraints**: The allowed values are **Personal** or **Web Hosting**.
certificateLocation	(Optional) When the locationType "File system" is chosen, the certificateLocation specifies the actual folder location where the PFX file should be placed. **Type**: String **Constraints**: It is applicable only if the IIS server is managed with the centralized "file system". If the certificateLocation is left blank, the location specified during IIS server device addition is taken as the location.
certificateFileName	(Mandatory) The "certificate friendly name" under which the certificate should be stored in the Certificate store. In the case of a file system, it is the "certificate file name" with which the certificate should be stored in the file system. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for IIS Server (continued)

Name	Description
	Constraints: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, .
bindType	(Optional) Specifies whether the binding type is Update certificate binding only, Create new site binding, or Update site binding (port, hostname, SNI). **Type**: String **Constraints**: It is applicable for locationType as "Certificate store". The allowed values are **Update certificate only**, **Update site binding**, and **Create new site binding**.
IsSNIEnabled	(Optional) The Server Name Indication option to be mapped in IIS site binding. **Type**: Boolean **Constraints**: It is applicable when bindType is **Update site binding** or **Create new site binding**. It is also applicable for IIS versions >= 8.0.
hostName	(Optional) The hostname of the server that has to be updated in the site binding. **Type**: String **Constraints**: It is applicable when bindType is **Update site binding** or **Create new site binding**.
port	(Optional) The server port number that has to be updated in the site binding. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for IIS Server (continued)

Name	Description
	Constraints: • It is applicable when bindType is **Update site binding** or **Create new site binding**. • This field is **mandatory** for for bindType **Create new site binding**. • The allowed values are between 1-65535.
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Certificate details for Microsoft PC Server

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The allowed values are **PKCS12-.pfx**.
certificateFileName	(Mandatory) The "certificate friendly name" under which the certificate should be stored in the Certificate store. **Type**: String **Constraints**: The certificate file name should not start and end with special characters except @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, .
pfxPassword	(Mandatory) The temporary password used during a certificate push. **Type**: String **Constraints**: The value must be base64 encoded.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Microsoft PC Server (continued)

Name	Description
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Certificate details for Microsoft Server

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PEM-.crt**, **PEM-.cer**, **PEM-.pem**, **DER-.cer**, **DER-.der**, **JKS-.jks**, **PKCS7-.p7b**, **PKCS7-.p7c**, **PKCS12-.p12**, and **PKCS12-.pfx**.
pushLocation	(Mandatory) The folder location in which certificate and private key are pushed. **Type**: String
certificateFileName	(Mandatory) A user-defined file name for pushing the certificate into the Microsoft server. **Type**: String **Constraints**: The file name must be suffixed with the certificate format to be pushed e.g.: test.appviewx.com.pfx.
privateKeyFileName	(Mandatory) A user-defined file name for pushing the certificate into the Microsoft server. **Type**: String **Constraints**: The file name must be suffixed with the certificate format to be pushed, e.g.: test.appviewx.com.key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Microsoft Server (continued)

Name	Description
	It is only applicable for types **PEM-.crt**, **PEM-.cer**, **PEM-.pem**, **DER-.cer**, **DER-.der**, **PKCS7-.p7b**, and **PKCS7-.p7c**.
pfxPassword	(Optional) The password of pfx/p12 file. **Type**: String **Constraints**: The value must be base64 encoded. It is only applicable for types **PKCS12-pfx**, and **PKCS-p12**.
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is only applicable for **JKS-.jks**certificate type.
keyStorePassword	(Optional) The jks file password. **Type**: String **Constraints**: The value must be base64 encoded. It is only applicable for types **PKCS12-pfx**, and **PKCS-p12**.
privateKeyPassword	(Optional) The private key entry password for the jks file. **Type**: String **Constraints**: The value must be base64 encoded. It is only applicable for types **PKCS12-pfx**, and **PKCS-p12**.
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean **Constraints**:
rootCertificateFileName	(Mandatory) A user-defined file name for pushing the root certificate into the Microsoft server. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Microsoft Server (continued)

Name	Description
	Constraints: The root certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The root certificate file name should also be different from both the CA file name and the intermediate certificate file name.
intermediateCertificateFileName	(Mandatory) A user-defined file name for pushing the intermediate certificate into the Microsoft server. **Type**: String **Constraints**: The intermediate certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The intermediate certificate file name should also be different from both the certificate file name and the CA file name.

Certificate details for Apache (Linux) Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PEM-.crt**, **PEM-.cer**, and **PEM-.pem**.
certificateLocation	(Mandatory) User-defined location (including the directory name and file name) for the certificate to be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Apache (Linux) Server (continued)

Name	Description
	Constraints: The certificate file name should not begin or end with special characters except -, ., _. The CA file name should also be different from both the CA file name and the intermediate certificate file name.
keyLocation	(Mandatory) User defined location, including both, the directory and file name, for pushing the keys into the Tomcat Linux server **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. . The private key file name should be same as the certificateFileName.
isRestartRequired	(Optional) Option to restart the service after the push operation. **Type**: Boolean
pushRootAndIntermediateCertificates	(Mandatory) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
trustLocation	(Mandatory) A user-defined directory for pushing the root and intermediate certificate into the Apache server. **Type**: String **Constraints**: The root certificate file name should not begin or end with special characters. The special characters allowed are !, @, #, $, %, ^, &, _, {, }, [,], |, :, <, >, (,), ;, . The CA file name should also be different from both the certificate file name and the CA file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Apache server. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Apache (Linux) Server (continued)

Name	Description
	Constraints: Mandatory when "pushRootAndIntermediateCertificates" is true. The root certificate file or bundle name should not begin or end with special characters. The special characters allowed are -, _, .. The root certificate file name should also be different from the certificate and intermediate certificate file name.
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the Apache server. **Type**: String **Constraints**: Mandatory when "pushRootAndIntermediateCertificates" is true. The intermediate certificate file or bundle name should not begin or end with special characters. The special characters allowed are -, _, .. The intermediate certificate file name should also be different from the certificate and root certificate file name.
privateKeyInDevice	(Optional) Determines whether users need to push the private key into the device. **Type**: Boolean

Certificate details for Tomcat (Linux) Server

Name	Description
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PEM-.crt**, **PEM-.cer**, **PEM-.pem**, and **JKS-.jks**.
certificateLocation	(Mandatory) User-defined location (including the directory name and file name) for the certificate to be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Tomcat (Linux) Server (continued)

Name	Description
	Type: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The CA file name should also be different from both the CA file name and the intermediate certificate file name.
keyLocation	(Mandatory) User defined location, including both, the directory and file name, for pushing the keys into the Tomcat Linux server **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. . The private key file name should be same as the certificateFileName.
keyStoreLocation	(Mandatory) A user-defined store location for pushing the keys and certificates into the Tomcat server. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**. Enter the keystore location with the extension as **.jks** or **.keystore**.
keyStorePassword	(Mandatory) The .jks file password. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Tomcat (Linux) Server (continued)

Name	Description
	Constraints: It is applicable for certificate type **JKS-.jks**.
privateKeyLocation	(Optional) A user-defined directory for pushing the private keys into the Tomcat server. **Type**: String **Constraints**: It is mandatory if “privateKeyInDevice” is true and is applicable only for certificate type **JKS-.jks**.
pushRootAndIntermediateCertificates	(Optional) Determines whether the root and intermediate certificate needs to be pushed to the device. **Type**: Boolean **Constraints**: It is applicable for all certificate types.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Tomcat server. **Type**: String **Constraints**: Mandatory when “pushRootAndIntermediateCertificates” is true. The root certificate file or bundle name should not begin or end with special characters except -, _, .. The root certificate file name should also be different from the certificate and intermediate certificate file name.
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the Apache server. **Type**: String **Constraints**: Mandatory when “pushRootAndIntermediateCertificates” is true. The intermediate certificate file or bundle name should not begin or end with special characters except -, _, .. The intermediate certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Tomcat (Linux) Server (continued)

Name	Description
	file name should also be different from the certificate and root certificate file name.
trustStoreLocation	(Optional) A user-defined store location for pushing the CA certificates into the device. **Type**: String **Constraints**: Mandatory when “pushRootAndIntermediateCertificates” is true. It is applicable for certificate type JKS-.jks. Provide the truststore location with the extension as **.jks** or **.truststore**.
trustStorePassword	(Optional) The .jks file password. **Type**: String **Constraints**: It is applicable for certificate type JKS-.jks.

Certificate details for Websphere Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **JKS-.jks**, and **PKCS12-.p12**.
keyStoreLocation	(Mandatory) A user-defined store location for pushing the keys and certificates into the server device. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Websphere Server (continued)

Name	Description
	Constraints: Enter the keystore location with the extension as **.jks** or **.keystore**.
keyStorePassword	(Optional) The jks file password. **Type**: String **Constraints**: Keystore password must have at least 6 characters.
trustStoreLocation	(Mandatory) A user-defined store location for pushing the CA certificates into the server device. **Type**: String **Constraints**: Provide the truststore location with the extension as **.jks** or **.truststore**. It is applicable only for certificate type JKS-.jks.
trustStorePassword	(Optional) The .jks file password. **Type**: String **Constraints**: Truststore password must have at least 6 characters. It is applicable only for certificate type JKS-.jks.
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean
keyLocation	(Optional) A user-defined key directory name for pushing the keys into the server device. **Type**: String
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Weblogic Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **JKS-.jks**.
keyStoreLocation	(Mandatory) A user-defined store location for pushing the keys and certificates into the server device. **Type**: String **Constraints**: Enter the keystore location with the extension as **.jks** or **.keystore**.
keyStorePassword	(Optional) The jks file password. **Type**: String **Constraints**: Keystore password must have at least 6 characters.
trustStoreLocation	(Mandatory) A user-defined store location for pushing the CA certificates into the server device. **Type**: String **Constraints**: Provide the truststore location with the extension as **.jks** or **.truststore**. It is applicable only for certificate type JKS-.jks.
trustStorePassword	(Optional) The .jks file password. **Type**: String **Constraints**: Truststore password must have at least 6 characters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Weblogic Server (continued)

Name	Description
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean
keyLocation	(Optional) A user-defined key directory name for pushing the keys into the server device. **Type**: String
aliasName	(Optional) The end entity certificate alias name for the jks file. **Type**: String **Constraints**: It is applicable for certificate type **JKS-.jks**.

Certificate details for IPlanet Server

Name	Description
isManualPush	(Optional) If selected, users can customize the certificate and key push locations. **Type**: Boolean
certificateType	(Mandatory) Certificate type i.e. the format in which the certificate is to be pushed to the server device. **Type**: String **Constraints**: The possible values are **PKCS12-.pfx**.
dbPath	(Mandatory) The database location for pushing the certificates into the server device. **Type**: String
dbPassword	(Optional) Password required to import certificates to database in server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for IPlanet Server (continued)

Name	Description
	Type: String
isRestartRequired	(Optional) Option to restart the service after the push operation. **Type**: Boolean
privateKeyInDevice	(Optional) Determines whether the private key needs to be pushed to the device. **Type**: Boolean
keyLocation	(Optional) A user-defined key directory name for pushing the keys into the server device. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
requestId response	Request Id for push action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	selectedProfiles parameter is already available in the specified certificate. **Remediation**: Provide a different value for the selectedProfiles field.
404 Not Found	NO_RECORDS_FOUND	No matching records found - certificate not found. **Remediation**: Provide a correct value for the field certificateId.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0016	Connector with profiles {} already exists. **Remediation**: A profile connector is already available for the selected certificate. Change the certificateId or delete the existing connector.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload


```
{
 "certificateDetails": {
 "certificateType": "PEM-.pem",
 "certificateName": "testfile",
 "pushRootAndIntermediateCertificates": true,
 "rootCertificateFileName": "testrootfile.pem",
 "intermediateCertificateFileName": [
 "testinterfilelevel1.pem"
 ]
 },
 "pushDetails": {
 "preValidationScriptPath": "",
 "postValidationScriptPath": "",
 "overwrite": false,
 "pushAutomatically": false
 },
 "certificateId": "5f5b1fac77534426423bab57",
 "selectedProfiles": [
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST"

]

}
```


Response


```
{

"response": [

{

"requestId": "3",

"connectorId": "xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST:@389ed6f96387e3002cc6ac0678c07ffe70459abf"

}

],

"message": "1 connector(s) saved and push operation has been triggered.",

"appStatusCode": null,

"tags": {},

"headers": null

}
```


Sample Request/Response for Apache (Linux) Server

Request Payload


```
{

"certificateDetails": {

  "useExistingConfiguration": false,

  "certificateType": "PEM-.crt",

  "certificateLocation": "/home/appviewx/server_03122024.crt",

  "keyLocation": "/tmp/apache/test.key",

  "isRestartRequired": false,

  "pushRootAndIntermediateCertificates": false,

  "privateKeyInDevice": false,

  "privateKeyLocation": "",

  "certificateTags": {},

  "intermediateCertificateFileName": []

 },

"certificateId": "605dbd66ccb1c49e108e67e6",

"selectedProfiles": [

"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf"

]

}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response


```
{
"response":[
{
"requestId":"54",
"connectorId":"ApacheLinux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf:@51fb6d24534926ea1d89d32bfe59b25c26d84b
5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for all three certificate types (PEM-.crt, PEM-.cer, PEM-.pem) for the Apache server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for IPlanet Server

Request Payload


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "PKCS12-.pfx",
"dbPath": "/opt/automation/db",
"dbPassword": "YXBwd==26",
"isRestartRequired":false,
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"iPlanet:@8443:@localhost:@localhost:"
]
}
```


Response


```
{
"response":[
{
"requestId":"60",
"connectorId":"iPlanet:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed PKCS12 certificate type (PKCS12-.pfx) for the IPlanet server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for Tomcat (Linux) Server

Request Payload


```
{
"certificateDetails": {
  "useExistingConfiguration": false,
  "certificateType": "PEM-.crt",
  "certificateLocation": "/home/appviewx/server_03122024.crt",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "keyLocation": "/tmp/tomcat/test.key",
  "isRestartRequired": false,
  "pushRootAndIntermediateCertificates": false,
  "privateKeyInDevice": false,
  "privateKeyLocation": "",
  "certificateTags": {},
  "intermediateCertificateFileName": []
 },
"pushDetails": {
   "preValidationScriptPath": "",
   "postValidationScriptPath": "",
   "overwrite": false,
   "pushAutomatically": false
},
"certificateId": "5f5b1fac77534426423bab57",
"selectedProfiles": [
"xxx.xxx.xx.xxx:@Template_001:@shared:@IKE Gateway Profile:@TEST"
]
}
```


Response


```
{
"response":[
{
"requestId":"57",
"connectorId":"TomcatLinux:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- The above sample request and response can be followed for all three certificate types (PEM-.crt, PEM-.cer, PEM-.pem) for the Tomcat server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for Weblogic Server

Sample Request


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "JKS-.jks",
"keyStoreLocation": "/opt/automation/key.jks",
"keyStorePassword": "YXBwd==26",
"trustStoreLocation": "/opt/automation/trust.jks",
"trustStorePassword": "YXBwd==26"
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
"aliasName": "sampleKeystore"
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"Weblogic:@8443:@localhost:@localhost:"
]
}
```


Sample Response


```
{
"response":[
{
"requestId":"58",
"connectorId":"Weblogic:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for JKS certificate type (JKS.jks) for the Websphere server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Sample Request/Response for Websphere Server

Request Payload


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "JKS-.jks",
"keyStoreLocation": "/opt/automation/key.jks",
"keyStorePassword": "YXBwd==26",
"trustStoreLocation": "/opt/automation/trust.jks",
"trustStorePassword": "YXBwd==26"
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
"aliasName": "sampleKeystore"
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"WebsphereLinux:@8443:@localhost:@localhost:"
]
}
```


Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
"response":[
{
"requestId":"58",
"connectorId":"WebsphereLinux:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for JKS certificate type (JKS.jks) for the Websphere server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

Request Payload


```
{
"certificateDetails": {
"isManualPush":true,
"certificateType": "PKCS12-.p12",
"keyStoreLocation": "/opt/automation/key.jks",
"keyStorePassword": "YXBwd==26",
"privateKeyInDevice": true,
"privateKeyLocation":"/opt/automation/keys",
"aliasName": "sampleKeystore"
},
"pushDetails": {
"preValidationScriptPath": "",
"postValidationScriptPath": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"pushAutomatically": false
},
"certificateId": "605dbd66ccb1c49e108e67e6",
"selectedProfiles": [
"WebsphereLinux:@8443:@localhost:@localhost:"
]
}
```


Response


```
{
"response":[
{
"requestId":"59",
"connectorId":"WebsphereLinux:@8443:@localhost:@localhost:@51fb6d24534926ea1d89d32bfe59b25c26d84b5e"
}
],
"message":"1 connector(s) saved and push operation has been triggered.",
"appStatusCode":null,
"tags":{
},
"headers":null
}
```


Note:

- The above sample request and response can be followed for PKCS12 certificate type (PKCS12-.p12) for the Websphere server.
- The **certificateId** in the above request can be found using the search API with parameters such as commonName, serialNumber or other search parameters.
- The **resourceId** present in Search API response is equivalent to the **certificateId** here.

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Rollback Certificate to Server Profile

The rollback certificate to a server profile API rolls back the certificate and its private keys to the server profile and links them to the server profiles. Refer to the After you are done section to Approve and Implement the request.

Before you begin

Ensure the following before attempting to rollback certificate to a server profile through AppViewX:

- Server devices must be configured in AppViewX.
- The devices should be in Managed state.
- **Approval is not required:** Enable this mode by setting the ‘Certificate Requests Need Approval?’ flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/rollback
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/rollback?gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
autoApproval *Query*	(Mandatory) Indicates whether the auto-approval is needed for the action. **Type**: String **Constraint**: Value of the parameter should be **yes**.
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
applicationConnectorIds	(Mandatory) Application connector id. **Type**: List <String>

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
requestId response	Request Id for rollback action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success message or failure description in case of error. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	App connector rollback action initiated for 1 connector(s).
202 Accepted	NA	Operation cannot be completed for one or more devices as the 'Resource' allocated to you does not have write permission. **Remediation**: Ensure that users have access to the device.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0012	Application connector ids cannot be empty. **Remediation**: Please provide value for the field applicationConnectorIds.
417 Expectation failed	ERR_APPLICATION_CONNECTOR_LIST_RETRIVAL	Unable to retrieve connector information. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_APP_CONNECTORS_NOT_FOUND	Application connector(s) not found. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_INITIALIZE_ROLLBACK_REQUEST	Unable to initialize rollback request.
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "applicationConnectorIds": [ "xx.xxx:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
 }
```


Note: Please refer to the "Request Structure" to identify the changeable values.

Response


```
{
"response": [
{
"requestId": "246",
"connectorId":
 "apache_linux:@/etc/apache2:@_default_:@443:@/etc/apache2/sites-available/default-ssl.conf:@7d741b31b872dca2e2bfb05d2181212f138455a6"
}
],
"message": "App connector rollback action initiated for 1 connector(s).",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Delete Certificate using UUID

The delete certificate using UUID API deletes the certificates using the Universal Unique Identifier (UUID). The UUID is a unique id for each certificate. This id remains the same even if the certificate is generated numerous times. It is generated based on certain attributes and properties of the certificate.

Request Structure

Endpoint:	/certificate/delete
Type:	DELETE
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/delete?gwsource=external&commonName={commonName}&serialNumber={serialNumber}` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username	(Mandatory) AppViewX login username.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
certIds	(Mandatory) Format required. **Type**: Array **Constraint**: Uuid of the certificate to be deleted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Error Response Parameters

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-CA-0047	Cert Ids cannot be empty. **Remediation**: Provide UUIDs in the request to delete certificates.
417 Expectation failed	CERT-HLST-0019	The operation cannot be completed as {} selected certificate(s) are in Read-Only access groups. **Remediation**: Change the permissions in the required access group.
400 Not Found	CERT-INV-0021	Requested certificate is not available in the inventory. **Remediation**: Provide uuids that are available in the inventory.
500 Internal Server Error	CERT-GEN-0028	Certificate Limit Exceed. **Remediation**: Cannot delete more than 100 certificates.

Sample Request/Response

Request Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

No payload for DELETE request.

Success Response


```
{
 {
 "response": {
 "code": "CERTIFICATE_DELETION_SUCCESSFULL",
 "message": "Selected certificate(s) has been deleted successfully from AppViewX inventory."
 },
 "message": null,
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Discover Certificates from Firewall

The API will discover certificates and it's private keys from the firewall device.

Before you begin

Ensure the following before attempting to discover a certificate from a particular firewall device through AppViewX:

- Firewall devices should be added in AppViewX.
- The device should be in Managed state.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/action?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String **Possible values:**: ONDEMAND, SCHEDULED
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
description	(Optional) Description of the discovery request. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: String **Constraint**: Not mandatory if the field **rbacRuleProcessRequired** is **true**
source	(Mandatory) Source of the certificates. **Type**: String **Possible values:**: Value should be **FIREWALL**.
certStatus	(Mandatory) Specifies the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: Managed, Monitored, or None. If "None", then certificates will not be moved to certificate inventory.
targetList	(Mandatory) Name of the devices where the certificates need to be discovered. **Type**: List of String **Constraint**: Device names which are added already need to be specified.
coolingPeriod	(Mandatory) Indicates whether the discovery is sequential or parallel. 0 is for sequential, whereas 1< indicates parallel. **Type**: Integer
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Rule name which is added already need to be specified.
rbacRuleProcessRequired	(Optional) Determines whether Rbac rule process is required. **Type**: Boolean (true or false) **Constraint**: If "true", then new certificates will be tagged under the group specified in the rule.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message response	Success message of the action or failure description in case of error. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: Object
header	HTTP headers associated with the response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found. **Remediation**: Ensure that a valid value is provided for the targetList field in the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1. **Remediation**: Provide a correct value in the field coolingPeriod.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Sample Request


```
{
"discoveryType": "ONDEMAND",
"name": "ServerDiscovery",
"description": "Discovery from server devices",
"source": "SERVER",
"coolingPeriod": "5",
"associatedRule": "RevokedCertExclusion",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"certStatus": "MANAGED",
"rbacRuleProcessRequired": false,
"groupName": "Default",
"targetList": [
"ApacheLinux"
]
}
```


Sample Response


```
{
"response": {
"discoveryName": "ServerDiscovery",
"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered."
},
"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Discover Certificates from Server

The API will discover certificates and their private keys from the server device.

Before you begin

Ensure the following before attempting to discover a certificate from a particular server device through AppViewX:

- Server devices should be added in AppViewX.
- The device should be in Managed state.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.
Header	**Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String **Possible values:**: ONDEMAND, SCHEDULED
name	(Mandatory) Name of the discovery instance to be created.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
description	(Optional) Description of the discovery request. **Type**: String
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: String **Constraint**: Not mandatory if the field **rbacRuleProcessRequired** is **true**
source	(Mandatory) Source of the certificates. **Type**: String **Possible values:**: Server
certStatus	(Mandatory) Specifies the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: Managed, Monitored, or None. If "None", then certificates will not be moved to certificate inventory.
targetList	(Mandatory) Name of the devices where the certificates need to be discovered. **Type**: List of String **Constraint**: Device names which are added already need to be specified.
coolingPeriod	(Mandatory) Indicates whether the discovery is sequential or parallel. 0 is for sequential, whereas 1< indicates parallel. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String **Constraint**: Rule name which is added already need to be specified.
rbacRuleProcessRequired	(Optional) Determines whether Rbac rule process is required. **Type**: Boolean (true or false) **Constraint**: If "true", then new certificates will be tagged under the group specified in the rule.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message response	Success message of the action or failure description in case of error. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of a failure response. **Type**: Object
header	HTTP headers associated with the response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the targetList field in the request.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1. **Remediation**: Provide a correct value in the field coolingPeriod.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Sample Request

```
{
"discoveryType": "ONDEMAND",
"name": "ServerDiscovery",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"description": "Discovery from server devices",
"source": "SERVER",
"coolingPeriod": "5",
"associatedRule": "RevokedCertExclusion",
"certStatus": "MANAGED",
"rbacRuleProcessRequired": false,
"groupName": "Default",
"targetList": [
"ApacheLinux"
]
}
```


Sample Response


```
{
"response": {
"discoveryName": "ServerDiscovery",
"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered."
},
"message": "Discovery history details added successfully with discovery id 605dc592c0bb5b1924e6851f, and discovery operation has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Discover Certificates from CT Log

The API will discover certificates from CT log.

Before you begin

Ensure that the provided domains are valid.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Required if username and password are not provided.
username	(Mandatory) AppViewX login username. *Header* **Type**: String **Constraint**: Required if sessionId is not provided.
password	(Mandatory) AppViewX login password. *Header* **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type	(Mandatory) Specifies the nature of the data in the payload. *Header* **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource	(Mandatory) Source from which the request is triggered. (E.g. external) *Query* **Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request. *Body* **Type**: Payload

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String **Possible values:**: ONDEMAND

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
description	(Optional) Description of the discovery request. **Type**: String
source	(Mandatory) Network source to discover certificates from **Type**: String **Important**: The values are case-sensitive. **Possible value(s):**: IPRANGE, SUBNET, URL
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String **Constraint**: Rule name which is added already need to be specified.
certStatus	(Mandatory) Specify the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: MANAGED, MONITERED, NONE (the values are case sensitive) **Important**: The values are case-sensitive. If **certStatus** = **NONE**, the discovered certificates will not be moved to certificate inventory.
rbacRuleProcessRequired	(Optional) Specify whether RBAC rule process is required. **Type**: Boolean (true or false) **Constraint**: If this is set to **true**, new certificates will be tagged under the group specified in the rule.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: domainList
domainList	(Mandatory) List of the domains to be scanned. **Type**: String
occuranceType	(Mandatory) Occurrence frequency **Type**: String **Possible values:**: DAILY, WEEKLY, MONTHLY, YEARLY
neverEnds	(Mandatory) Specify if the discovery should be a never ending occurrence **Type**: Boolean **Possible value(s):**: true, false
startDate	(Mandatory if **discoveryType** = **SCHEDULED**) Start date for the scheduled network discovery scan **Type**: Long
timeZone	(Mandatory if **discoveryType** = **SCHEDULED**) Time zone in which the scheduled network discovery scan will be triggered **Type**: String **Possible values:**: Possible values for time zone
endDate	(Optional - Applicable for discoveryType = SCHEDULED). End date for the scheduled network discovery scan. **Type**: Long
endAfterNoOfOccurances	(Optional - Applicable for discoveryType = SCHEDULED). Number of occurrences after which the scheduled network discovery scan is ended.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Integer
occuranceDays	(Optional - Applicable for discoveryType = SCHEDULED AND occuranceType = WEEKLY). List of days of week in which the scheduled discovery to be triggered. **Type**: List **Possible Value**: MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY **Default Value**: MONDAY

Note: If endAfterNoOfOccurances is null or 0, and endDate is null, and neverEnds is either null or false, then neverEnds will be automatically set to true.

Payload-DomainList

Name	Description
domainName	(Mandatory) domain name for the CT Log discovery.\ **Type**: String
dataCenter	(Mandatory) The data center for the domain. **Type**: String **Constraint**: The provided dataCenter must be available.

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message response	Success message of the action or failure description in case of error. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object
header	HTTP headers associated with the response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found. **Remediation**: Ensure that a valid value is provided for the targetList field in the request.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1. **Remediation**: Provide a correct value in the field coolingPeriod.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Sample Request

```
{
    "discoveryType": "ONDEMAND",
    "name": "on_demand_network",
    "description": "on_demand_network desc",
    "source": "NETWORK",
    "groupName": "Default",
    "networkList" : [
"BLR_network"
    ],
    "certStatus": "NONE",
    "rbacRuleProcessRequired" : false,
    "associatedRule": "ignore_revoked_certs"
}
```

Sample Request

```
{
    "discoveryType": "SCHEDULED",
    "name": "scheduled_network",
    "description": "scheduled_network desc",
    "source": "NETWORK",
    "groupName": "Default",
    "networkList" : [
        "BLR_network"
    ],
    "certStatus": "MANAGED",
    "rbacRuleProcessRequired" : false,
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "associatedRule": "ignore_revoked_certs",
  "occuranceType": "WEEKLY",
  "occuranceDays": ["TUESDAY", "WEDNESDAY"],
  "neverEnds": true,
  "startDate": 1749555000000,
  "hostNames": "appviewx.com",
  "passiveMode": false,
  "fullScanAfterNumberOfPassiveDiscoveries": 0,
  "timeZone":"Asia/Calcutta"
}
```


Sample Response


```
{
  "response": {
     "discoveryName": "on_demand_network",
     "message": "Discovery history details added successfully with discovery id 683d53800b80a91c95bee4da, and discovery operation has been triggered."
  },
  "message": "Discovery history details added successfully with discovery id 683d53800b80a91c95bee4da, and discovery operation has been triggered.",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Possible time zone values

Etc/GMT+12

Pacific/Pago_Pago

Pacific/Samoa

Pacific/Niue

US/Samoa

Etc/GMT+11

Pacific/Midway

Pacific/Honolulu

Pacific/Rarotonga

Pacific/Tahiti

Pacific/Johnston

America/Atka

US/Hawaii

SystemV/HST10

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Adak

US/Aleutian

Etc/GMT+10

Pacific/Marquesas

Etc/GMT+9

US/Alaska

America/Juneau

America/Metlakatla

Pacific/Gambier

America/Yakutat

America/Sitka

SystemV/YST9

America/Anchorage

America/Nome

SystemV/YST9YDT

Etc/GMT+8

Canada/Pacific

PST8PDT

Pacific/Pitcairn

Mexico/BajaNorte

America/Tijuana

SystemV/PST8

America/Santa_Isabel

America/Vancouver

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Ensenada

SystemV/PST8PDT

America/Los_Angeles

US/Pacific

Canada/Yukon

Etc/GMT+7

US/Arizona

Mexico/BajaSur

America/Dawson_Creek

America/Denver

America/Yellowknife

America/Inuvik

America/Ciudad_Juarez

America/Mazatlan

SystemV/MST7

America/Boise

America/Dawson

MST7MDT

US/Mountain

America/Creston

America/Edmonton

America/Hermosillo

Canada/Mountain

America/Cambridge_Bay

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Navajo

America/Phoenix

America/Whitehorse

SystemV/MST7MDT

America/Fort_Nelson

America/Shiprock

America/El_Salvador

America/Guatemala

America/Belize

America/Managua

America/Chicago

America/Tegucigalpa

Etc/GMT+6

America/Regina

Mexico/General

America/Rankin_Inlet

US/Central

Pacific/Galapagos

America/Rainy_River

America/Swift_Current

America/Costa_Rica

America/Indiana/Knox

America/North_Dakota/Beulah

America/Monterrey

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

SystemV/CST6

America/North_Dakota/Center

America/Indiana/Tell_City

America/Chihuahua

America/Ojinaga

America/Mexico_City

America/Matamoros

CST6CDT

America/Knox_IN

America/Menominee

America/Resolute

Canada/Central

America/Bahia_Banderas

US/Indiana-Starke

SystemV/CST6CDT

America/Merida

Canada/Saskatchewan

America/North_Dakota/New_Salem

America/Winnipeg

America/Panama

America/Indiana/Petersburg

America/Eirunepe

America/Grand_Turk

Cuba

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Etc/GMT+5

Pacific/Easter

America/Fort_Wayne

America/Havana

America/Porto_Acre

US/Michigan

America/Louisville

America/Guayaquil

America/Indiana/Vevay

America/Indiana/Vincennes

America/Indianapolis

America/Iqaluit

America/Kentucky/Louisville

EST5EDT

America/Nassau

America/Jamaica

America/Atikokan

America/Kentucky/Monticello

America/Coral_Harbour

America/Cayman

Chile/EasterIsland

America/Indiana/Indianapolis

America/Thunder_Bay

America/Indiana/Marengo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Bogota

SystemV/EST5

US/Eastern

Canada/Eastern

America/Port-au-Prince

America/Nipigon

Brazil/Acre

US/East-Indiana

America/Cancun

America/Lima

America/Rio_Branco

America/Detroit

Jamaica

America/Pangnirtung

America/Montreal

America/Indiana/Winamac

America/New_York

America/Toronto

SystemV/EST5EDT

America/Cuiaba

America/Marigot

Canada/Atlantic

Etc/GMT+4

America/Manaus

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/St_Thomas

America/Anguilla

America/Barbados

America/Curacao

America/Guyana

America/Martinique

America/Puerto_Rico

America/Port_of_Spain

SystemV/AST4

America/Kralendijk

America/Antigua

America/Moncton

America/St_Vincent

America/Dominica

Atlantic/Bermuda

Brazil/West

America/Aruba

America/Halifax

America/La_Paz

America/Blanc-Sablon

America/Santo_Domingo

America/Glace_Bay

America/St_Barthelemy

America/St_Lucia

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Montserrat

America/Lower_Princes

America/Thule

America/Tortola

America/Porto_Velho

America/Campo_Grande

America/Goose_Bay

America/Virgin

America/Boa_Vista

America/Grenada

America/St_Kitts

America/Caracas

America/Guadeloupe

SystemV/AST4ADT

America/St_Johns

Canada/Newfoundland

Chile/Continental

America/Miquelon

America/Argentina/Catamarca

America/Argentina/Cordoba

America/Araguaina

America/Argentina/Salta

Etc/GMT+3

America/Montevideo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Brazil/East

America/Argentina/Mendoza

America/Argentina/Rio_Gallegos

America/Catamarca

America/Cordoba

America/Sao_Paulo

America/Argentina/Jujuy

America/Cayenne

America/Recife

America/Buenos_Aires

America/Paramaribo

America/Mendoza

America/Santarem

America/Asuncion

America/Maceio

Atlantic/Stanley

Antarctica/Rothera

America/Argentina/San_Luis

America/Santiago

America/Argentina/Ushuaia

Antarctica/Palmer

America/Punta_Arenas

America/Fortaleza

America/Argentina/La_Rioja

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Belem

America/Jujuy

America/Bahia

America/Argentina/San_Juan

America/Argentina/ComodRivadavia

America/Argentina/Tucuman

America/Rosario

America/Argentina/Buenos_Aires

Etc/GMT+2

America/Godthab

America/Noronha

Brazil/DeNoronha

Atlantic/South_Georgia

America/Scoresbysund

America/Nuuk

Etc/GMT+1

Atlantic/Cape_Verde

Atlantic/Azores

Pacific/Kiritimati

Etc/GMT-14

NZ-CHAT

Pacific/Chatham

Pacific/Fakaofo

Antarctica/McMurdo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Enderbury

NZ

Pacific/Apia

Antarctica/South_Pole

Pacific/Kanton

Pacific/Auckland

Pacific/Tongatapu

Etc/GMT-13

Pacific/Kwajalein

Pacific/Wallis

Pacific/Fiji

Pacific/Funafuti

Pacific/Nauru

Kwajalein

Pacific/Wake

Pacific/Norfolk

Pacific/Tarawa

Asia/Kamchatka

Etc/GMT-12

Asia/Anadyr

Pacific/Majuro

Australia/Hobart

Australia/Tasmania

Australia/ACT

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Ponape

Pacific/Bougainville

Australia/Victoria

Antarctica/Macquarie

Australia/Canberra

Australia/Currie

Australia/Lord_Howe

Australia/NSW

Pacific/Pohnpei

Pacific/Efate

Asia/Magadan

Pacific/Kosrae

Australia/Sydney

Australia/LHI

Asia/Sakhalin

Pacific/Noumea

Etc/GMT-11

Asia/Srednekolymsk

Australia/Melbourne

Pacific/Guadalcanal

Australia/Yancowinna

Australia/Adelaide

Australia/Broken_Hill

Australia/South

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Yap

Pacific/Port_Moresby

Pacific/Chuuk

Australia/Queensland

Pacific/Guam

Pacific/Truk

Asia/Vladivostok

Pacific/Saipan

Antarctica/DumontDUrville

Australia/Brisbane

Etc/GMT-10

Asia/Ust-Nera

Australia/Lindeman

Australia/North

Australia/Darwin

Etc/GMT-9

Pacific/Palau

Asia/Chita

Asia/Dili

Asia/Jayapura

Asia/Yakutsk

Asia/Pyongyang

ROK

Asia/Seoul

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Khandyga

Japan

Asia/Tokyo

Australia/Eucla

Asia/Kuching

Asia/Chungking

Etc/GMT-8

Australia/Perth

Asia/Macao

Asia/Macau

Asia/Choibalsan

Asia/Shanghai

Antarctica/Casey

Asia/Ulan_Bator

Asia/Chongqing

Asia/Ulaanbaatar

Asia/Taipei

Asia/Manila

PRC

Asia/Ujung_Pandang

Asia/Harbin

Singapore

Asia/Brunei

Australia/West

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Hong_Kong

Asia/Makassar

Hongkong

Asia/Kuala_Lumpur

Asia/Irkutsk

Asia/Singapore

Asia/Pontianak

Etc/GMT-7

Asia/Phnom_Penh

Asia/Novosibirsk

Antarctica/Davis

Asia/Tomsk

Asia/Jakarta

Asia/Barnaul

Indian/Christmas

Asia/Ho_Chi_Minh

Asia/Hovd

Asia/Bangkok

Asia/Vientiane

Asia/Novokuznetsk

Asia/Krasnoyarsk

Asia/Saigon

Asia/Yangon

Asia/Rangoon

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Indian/Cocos

Asia/Kashgar

Etc/GMT-6

Asia/Dacca

Asia/Omsk

Asia/Dhaka

Indian/Chagos

Asia/Bishkek

Asia/Urumqi

Asia/Thimbu

Asia/Thimphu

Asia/Kathmandu

Asia/Katmandu

Asia/Kolkata

Asia/Colombo

Asia/Calcutta

Asia/Aqtau

Etc/GMT-5

Asia/Samarkand

Asia/Almaty

Asia/Karachi

Asia/Yekaterinburg

Asia/Dushanbe

Indian/Maldives

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Oral

Asia/Tashkent

Asia/Qostanay

Antarctica/Mawson

Asia/Qyzylorda

Asia/Aqtobe

Asia/Ashkhabad

Antarctica/Vostok

Asia/Ashgabat

Asia/Atyrau

Indian/Kerguelen

Asia/Kabul

Asia/Yerevan

Etc/GMT-4

Asia/Dubai

Indian/Reunion

Indian/Mauritius

Europe/Saratov

Europe/Samara

Indian/Mahe

Asia/Baku

Asia/Muscat

Europe/Astrakhan

Asia/Tbilisi

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Ulyanovsk

Iran

Asia/Tehran

Asia/Aden

Africa/Nairobi

Europe/Istanbul

Etc/GMT-3

Indian/Comoro

Antarctica/Syowa

Africa/Mogadishu

Africa/Asmera

Asia/Istanbul

Europe/Moscow

Africa/Djibouti

Europe/Simferopol

Africa/Asmara

Asia/Baghdad

Asia/Damascus

Africa/Dar_es_Salaam

Africa/Addis_Ababa

Asia/Riyadh

Asia/Kuwait

Europe/Kirov

Africa/Kampala

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Minsk

Asia/Qatar

Asia/Bahrain

Indian/Antananarivo

Indian/Mayotte

Europe/Volgograd

Turkey

W-SU

Asia/Amman

Africa/Cairo

Africa/Mbabane

Etc/GMT-2

Europe/Zaporozhye

Libya

Africa/Kigali

Africa/Tripoli

Israel

Europe/Kaliningrad

Africa/Windhoek

Europe/Bucharest

Europe/Mariehamn

Africa/Lubumbashi

Europe/Tiraspol

Europe/Chisinau

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Helsinki

Asia/Beirut

Asia/Tel_Aviv

Europe/Sofia

Africa/Gaborone

Asia/Gaza

Europe/Riga

Africa/Maputo

Europe/Uzhgorod

Asia/Jerusalem

Africa/Bujumbura

Europe/Kiev

Europe/Vilnius

Africa/Maseru

Africa/Blantyre

Africa/Lusaka

Africa/Harare

Europe/Tallinn

Africa/Khartoum

Africa/Johannesburg

Africa/Juba

Europe/Kyiv

Asia/Nicosia

Asia/Famagusta

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EET

Asia/Hebron

Egypt

Europe/Nicosia

Europe/Athens

Europe/Brussels

Europe/Warsaw

CET

Etc/GMT-1

Europe/Luxembourg

Africa/Tunis

Europe/Malta

Europe/Busingen

Africa/Malabo

Europe/Skopje

Europe/Sarajevo

Africa/Lagos

Europe/Rome

Africa/Algiers

Europe/Zurich

Europe/Gibraltar

Europe/Vaduz

Europe/Ljubljana

Europe/Berlin

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Stockholm

Europe/Budapest

Europe/Zagreb

Europe/Paris

Africa/Ndjamena

Africa/Ceuta

Europe/Prague

Europe/Copenhagen

Europe/Vienna

Europe/Tirane

MET

Europe/Amsterdam

Africa/Libreville

Africa/El_Aaiun

Europe/San_Marino

Africa/Douala

Africa/Brazzaville

Africa/Porto-Novo

Poland

Europe/Andorra

Europe/Oslo

Europe/Podgorica

Africa/Casablanca

Africa/Luanda

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Atlantic/Jan_Mayen

Africa/Kinshasa

Europe/Madrid

Africa/Bangui

Europe/Belgrade

Africa/Niamey

Europe/Bratislava

Arctic/Longyearbyen

Europe/Vatican

Europe/Monaco

Europe/London

GMT

Etc/GMT-0

Europe/Jersey

Atlantic/St_Helena

Europe/Guernsey

Europe/Isle_of_Man

Etc/GMT+0

Africa/Banjul

Etc/GMT

Africa/Freetown

GB-Eire

Africa/Bamako

GB

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Conakry

Portugal

Universal

Africa/Sao_Tome

Africa/Nouakchott

Antarctica/Troll

UTC

Etc/Universal

Atlantic/Faeroe

Africa/Abidjan

Eire

Africa/Accra

Atlantic/Faroe

Etc/UCT

GMT0

Europe/Dublin

Zulu

Africa/Ouagadougou

Atlantic/Reykjavik

Atlantic/Madeira

Etc/Zulu

Iceland

Europe/Lisbon

Atlantic/Canary

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Lome

Greenwich

Europe/Belfast

Etc/GMT0

America/Danmarkshavn

Africa/Dakar

Africa/Bissau

WET

Etc/Greenwich

Africa/Timbuktu

UCT

Africa/Monrovia

Etc/UTC

Discover Certificates from Network

- Discover Certificates from Subnet
- Discover Certificates from IP Range
- Discover Certificates from URL
- Discover Certificates from Network

Discover Certificates from Subnet

The API will discover certificates and their private keys from a subnet.

Before you begin

Ensure that the target IP addresses for the network scan are reachable.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Payload	Contains all the parameters to be sent in the request body for the post request.
Body	**Type**: Payload

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String **Possible values:**: ONDEMAND, SCHEDULED
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
description	(Optional) Description of the discovery request. **Type**: String
source	(Mandatory) Network source to discover certificates from **Type**: String **Possible value(s):**: IPRANGE, SUBNET, URL
executeBatchesSequentially	(Optional) Specify if the discovey operation for batches must be executed sequentially **Type**: Boolean **Possible value(s):**: true, false
coolingPeriod	(Mandatory) Indicates whether the discovery is sequential or parallel. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible value(s):: • 0 (for parallel discovery) • 1 < (for sequential discovery) **Note:** 1 is not a valid value for this parameter.
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String **Constraint**: Rule name which is added already need to be specified.
certStatus	(Mandatory) Specify the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: MANAGED, MONITERED, NONE (the values are case sensitive) If **certStatus** = **NONE**, the discovered certificates will not be moved to certificate inventory.
rbacRuleProcessRequired	(Optional) Specify whether RBAC rule process is required. **Type**: Boolean (true or false) **Constraint**: If this is set to **true**, new certificates will be tagged under the group specified in the rule.
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: String
category	(Mandatory) Certificate category **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values:: server, client, code-signing
subnets	(Mandatory) Details of the subnet to be scanned **Type**: subnets
occuranceType	(Mandatory) Occurrence frequency **Type**: String **Possible values:**: DAILY, WEEKLY, MONTHLY, YEARLY
neverEnds	(Mandatory) Specify if the discovery should be a never ending occurrence **Type**: Boolean **Possible value(s):**: true, false
startDate	(Mandatory if **discoveryType** = **SCHEDULED**) Start date for the scheduled network discovery scan **Type**: Long
timeZone	(Mandatory if **discoveryType** = **SCHEDULED**) Time zone in which the scheduled network discovery scan will be triggered **Type**: String **Possible values:**: Possible values for time zone

Payload-Subnets

Name	Description
subnetwork	(Mandatory) Subnet in CIDR notation **Type**: String
ports	(Mandatory) Target ports to scan **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload-Subnets (continued)

Name	Description
	Possible value(s):: all, comma-separated list of individual ports to be scanned
batchSeperationConstant	(Mandatory) Subnet mask for specifying the subnet division for scanning **Type**: String
dataCenter	(Mandatory) Data center where the subnet is located **Type**: String
hostNames	(Mandatory) SNI hostname to be used while retrieving the certificate **Type**: Array
tlsVersions	(Optional) List of TLS versions to be used while communicating with the IP(s) for certificate retrieval **Type**: Array
standardPorts	(Optional) Specify if only standard ports must be scanned **Type**: Boolean **Possible value(s):**: true, false

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message	Success message of the action or failure description in case of error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object
header	HTTP headers associated with the response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found. **Remediation**: Ensure that a valid value is provided for the targetList field in the request.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1. **Remediation**: Provide a correct value in the field coolingPeriod.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Sample Request


```
{
 "discoveryType": "SCHEDULED",
 "name": "Subnet_2",
 "description": "",
 "source": "SUBNET",
 "executeBatchesSequentially": false,
 "coolingPeriod": 0,
 "associatedRule": "exclude_expired",
 "certStatus": "NONE",
 "rbacRuleProcessRequired": false,
 "groupName": "Default",
 "category": "server",
 "subnets": [
  {
    "subnetwork" : "192.168.41.0/24",
    "ports": "443,8443",
    "batchSeperationConstant": "/26",
    "dataCenter": "absecon",
    "hostNames": [],
    "tlsVersions": [
      "TLSv1.2"
    ],
    "standardPorts": false
  },
  {
    "subnetwork" : "192.168.42.0/24",
    "ports": "21555",
    "batchSeperationConstant": "/24",
    "dataCenter": "absecon",
    "hostNames": [],
    "tlsVersions": [
      "TLSv1.3",
      "TLSv1.2",
      "TLSv1.1",
      "SSLv3"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    ],
    "standardPorts": true
  }
 ],
 "occuranceType":"DAILY",
 "neverEnds" : true,
 "startDate" : 1738048400000,
 "timeZone" : "Pacific/Midway"
}
```


Sample Response


```
{
  "response": {
    "discoveryName": "Subnet_Disc_sch1212",
    "message": "Discovery scheduler details added successfully with discovery id 67added2c4a3610e43e040b4"
  },
  "message": "Discovery scheduler details added successfully with discovery id 67added2c4a3610e43e040b4",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Possible time zone values

Etc/GMT+12

Pacific/Pago_Pago

Pacific/Samoa

Pacific/Niue

US/Samoa

Etc/GMT+11

Pacific/Midway

Pacific/Honolulu

Pacific/Rarotonga

Pacific/Tahiti

Pacific/Johnston

America/Atka

US/Hawaii

SystemV/HST10

America/Adak

US/Aleutian

Etc/GMT+10

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Marquesas

Etc/GMT+9

US/Alaska

America/Juneau

America/Metlakatla

Pacific/Gambier

America/Yakutat

America/Sitka

SystemV/YST9

America/Anchorage

America/Nome

SystemV/YST9YDT

Etc/GMT+8

Canada/Pacific

PST8PDT

Pacific/Pitcairn

Mexico/BajaNorte

America/Tijuana

SystemV/PST8

America/Santa_Isabel

America/Vancouver

America/Ensenada

SystemV/PST8PDT

America/Los_Angeles

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

US/Pacific

Canada/Yukon

Etc/GMT+7

US/Arizona

Mexico/BajaSur

America/Dawson_Creek

America/Denver

America/Yellowknife

America/Inuvik

America/Ciudad_Juarez

America/Mazatlan

SystemV/MST7

America/Boise

America/Dawson

MST7MDT

US/Mountain

America/Creston

America/Edmonton

America/Hermosillo

Canada/Mountain

America/Cambridge_Bay

Navajo

America/Phoenix

America/Whitehorse

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

SystemV/MST7MDT

America/Fort_Nelson

America/Shiprock

America/El_Salvador

America/Guatemala

America/Belize

America/Managua

America/Chicago

America/Tegucigalpa

Etc/GMT+6

America/Regina

Mexico/General

America/Rankin_Inlet

US/Central

Pacific/Galapagos

America/Rainy_River

America/Swift_Current

America/Costa_Rica

America/Indiana/Knox

America/North_Dakota/Beulah

America/Monterrey

SystemV/CST6

America/North_Dakota/Center

America/Indiana/Tell_City

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Chihuahua

America/Ojinaga

America/Mexico_City

America/Matamoros

CST6CDT

America/Knox_IN

America/Menominee

America/Resolute

Canada/Central

America/Bahia_Banderas

US/Indiana-Starke

SystemV/CST6CDT

America/Merida

Canada/Saskatchewan

America/North_Dakota/New_Salem

America/Winnipeg

America/Panama

America/Indiana/Petersburg

America/Eirunepe

America/Grand_Turk

Cuba

Etc/GMT+5

Pacific/Easter

America/Fort_Wayne

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Havana

America/Porto_Acre

US/Michigan

America/Louisville

America/Guayaquil

America/Indiana/Vevay

America/Indiana/Vincennes

America/Indianapolis

America/Iqaluit

America/Kentucky/Louisville

EST5EDT

America/Nassau

America/Jamaica

America/Atikokan

America/Kentucky/Monticello

America/Coral_Harbour

America/Cayman

Chile/EasterIsland

America/Indiana/Indianapolis

America/Thunder_Bay

America/Indiana/Marengo

America/Bogota

SystemV/EST5

US/Eastern

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Canada/Eastern

America/Port-au-Prince

America/Nipigon

Brazil/Acre

US/East-Indiana

America/Cancun

America/Lima

America/Rio_Branco

America/Detroit

Jamaica

America/Pangnirtung

America/Montreal

America/Indiana/Winamac

America/New_York

America/Toronto

SystemV/EST5EDT

America/Cuiaba

America/Marigot

Canada/Atlantic

Etc/GMT+4

America/Manaus

America/St_Thomas

America/Anguilla

America/Barbados

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Curacao

America/Guyana

America/Martinique

America/Puerto_Rico

America/Port_of_Spain

SystemV/AST4

America/Kralendijk

America/Antigua

America/Moncton

America/St_Vincent

America/Dominica

Atlantic/Bermuda

Brazil/West

America/Aruba

America/Halifax

America/La_Paz

America/Blanc-Sablon

America/Santo_Domingo

America/Glace_Bay

America/St_Barthelemy

America/St_Lucia

America/Montserrat

America/Lower_Princes

America/Thule

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Tortola

America/Porto_Velho

America/Campo_Grande

America/Goose_Bay

America/Virgin

America/Boa_Vista

America/Grenada

America/St_Kitts

America/Caracas

America/Guadeloupe

SystemV/AST4ADT

America/St_Johns

Canada/Newfoundland

Chile/Continental

America/Miquelon

America/Argentina/Catamarca

America/Argentina/Cordoba

America/Araguaina

America/Argentina/Salta

Etc/GMT+3

America/Montevideo

Brazil/East

America/Argentina/Mendoza

America/Argentina/Rio_Gallegos

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Catamarca

America/Cordoba

America/Sao_Paulo

America/Argentina/Jujuy

America/Cayenne

America/Recife

America/Buenos_Aires

America/Paramaribo

America/Mendoza

America/Santarem

America/Asuncion

America/Maceio

Atlantic/Stanley

Antarctica/Rothera

America/Argentina/San_Luis

America/Santiago

America/Argentina/Ushuaia

Antarctica/Palmer

America/Punta_Arenas

America/Fortaleza

America/Argentina/La_Rioja

America/Belem

America/Jujuy

America/Bahia

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Argentina/San_Juan

America/Argentina/ComodRivadavia

America/Argentina/Tucuman

America/Rosario

America/Argentina/Buenos_Aires

Etc/GMT+2

America/Godthab

America/Noronha

Brazil/DeNoronha

Atlantic/South_Georgia

America/Scoresbysund

America/Nuuk

Etc/GMT+1

Atlantic/Cape_Verde

Atlantic/Azores

Pacific/Kiritimati

Etc/GMT-14

NZ-CHAT

Pacific/Chatham

Pacific/Fakaofo

Antarctica/McMurdo

Pacific/Enderbury

NZ

Pacific/Apia

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Antarctica/South_Pole

Pacific/Kanton

Pacific/Auckland

Pacific/Tongatapu

Etc/GMT-13

Pacific/Kwajalein

Pacific/Wallis

Pacific/Fiji

Pacific/Funafuti

Pacific/Nauru

Kwajalein

Pacific/Wake

Pacific/Norfolk

Pacific/Tarawa

Asia/Kamchatka

Etc/GMT-12

Asia/Anadyr

Pacific/Majuro

Australia/Hobart

Australia/Tasmania

Australia/ACT

Pacific/Ponape

Pacific/Bougainville

Australia/Victoria

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Antarctica/Macquarie

Australia/Canberra

Australia/Currie

Australia/Lord_Howe

Australia/NSW

Pacific/Pohnpei

Pacific/Efate

Asia/Magadan

Pacific/Kosrae

Australia/Sydney

Australia/LHI

Asia/Sakhalin

Pacific/Noumea

Etc/GMT-11

Asia/Srednekolymsk

Australia/Melbourne

Pacific/Guadalcanal

Australia/Yancowinna

Australia/Adelaide

Australia/Broken_Hill

Australia/South

Pacific/Yap

Pacific/Port_Moresby

Pacific/Chuuk

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/Queensland

Pacific/Guam

Pacific/Truk

Asia/Vladivostok

Pacific/Saipan

Antarctica/DumontDUrville

Australia/Brisbane

Etc/GMT-10

Asia/Ust-Nera

Australia/Lindeman

Australia/North

Australia/Darwin

Etc/GMT-9

Pacific/Palau

Asia/Chita

Asia/Dili

Asia/Jayapura

Asia/Yakutsk

Asia/Pyongyang

ROK

Asia/Seoul

Asia/Khandyga

Japan

Asia/Tokyo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/Eucla

Asia/Kuching

Asia/Chungking

Etc/GMT-8

Australia/Perth

Asia/Macao

Asia/Macau

Asia/Choibalsan

Asia/Shanghai

Antarctica/Casey

Asia/Ulan_Bator

Asia/Chongqing

Asia/Ulaanbaatar

Asia/Taipei

Asia/Manila

PRC

Asia/Ujung_Pandang

Asia/Harbin

Singapore

Asia/Brunei

Australia/West

Asia/Hong_Kong

Asia/Makassar

Hongkong

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Kuala_Lumpur

Asia/Irkutsk

Asia/Singapore

Asia/Pontianak

Etc/GMT-7

Asia/Phnom_Penh

Asia/Novosibirsk

Antarctica/Davis

Asia/Tomsk

Asia/Jakarta

Asia/Barnaul

Indian/Christmas

Asia/Ho_Chi_Minh

Asia/Hovd

Asia/Bangkok

Asia/Vientiane

Asia/Novokuznetsk

Asia/Krasnoyarsk

Asia/Saigon

Asia/Yangon

Asia/Rangoon

Indian/Cocos

Asia/Kashgar

Etc/GMT-6

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Dacca

Asia/Omsk

Asia/Dhaka

Indian/Chagos

Asia/Bishkek

Asia/Urumqi

Asia/Thimbu

Asia/Thimphu

Asia/Kathmandu

Asia/Katmandu

Asia/Kolkata

Asia/Colombo

Asia/Calcutta

Asia/Aqtau

Etc/GMT-5

Asia/Samarkand

Asia/Almaty

Asia/Karachi

Asia/Yekaterinburg

Asia/Dushanbe

Indian/Maldives

Asia/Oral

Asia/Tashkent

Asia/Qostanay

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Antarctica/Mawson

Asia/Qyzylorda

Asia/Aqtobe

Asia/Ashkhabad

Antarctica/Vostok

Asia/Ashgabat

Asia/Atyrau

Indian/Kerguelen

Asia/Kabul

Asia/Yerevan

Etc/GMT-4

Asia/Dubai

Indian/Reunion

Indian/Mauritius

Europe/Saratov

Europe/Samara

Indian/Mahe

Asia/Baku

Asia/Muscat

Europe/Astrakhan

Asia/Tbilisi

Europe/Ulyanovsk

Iran

Asia/Tehran

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Aden

Africa/Nairobi

Europe/Istanbul

Etc/GMT-3

Indian/Comoro

Antarctica/Syowa

Africa/Mogadishu

Africa/Asmera

Asia/Istanbul

Europe/Moscow

Africa/Djibouti

Europe/Simferopol

Africa/Asmara

Asia/Baghdad

Asia/Damascus

Africa/Dar_es_Salaam

Africa/Addis_Ababa

Asia/Riyadh

Asia/Kuwait

Europe/Kirov

Africa/Kampala

Europe/Minsk

Asia/Qatar

Asia/Bahrain

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Indian/Antananarivo

Indian/Mayotte

Europe/Volgograd

Turkey

W-SU

Asia/Amman

Africa/Cairo

Africa/Mbabane

Etc/GMT-2

Europe/Zaporozhye

Libya

Africa/Kigali

Africa/Tripoli

Israel

Europe/Kaliningrad

Africa/Windhoek

Europe/Bucharest

Europe/Mariehamn

Africa/Lubumbashi

Europe/Tiraspol

Europe/Chisinau

Europe/Helsinki

Asia/Beirut

Asia/Tel_Aviv

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Sofia

Africa/Gaborone

Asia/Gaza

Europe/Riga

Africa/Maputo

Europe/Uzhgorod

Asia/Jerusalem

Africa/Bujumbura

Europe/Kiev

Europe/Vilnius

Africa/Maseru

Africa/Blantyre

Africa/Lusaka

Africa/Harare

Europe/Tallinn

Africa/Khartoum

Africa/Johannesburg

Africa/Juba

Europe/Kyiv

Asia/Nicosia

Asia/Famagusta

EET

Asia/Hebron

Egypt

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Nicosia

Europe/Athens

Europe/Brussels

Europe/Warsaw

CET

Etc/GMT-1

Europe/Luxembourg

Africa/Tunis

Europe/Malta

Europe/Busingen

Africa/Malabo

Europe/Skopje

Europe/Sarajevo

Africa/Lagos

Europe/Rome

Africa/Algiers

Europe/Zurich

Europe/Gibraltar

Europe/Vaduz

Europe/Ljubljana

Europe/Berlin

Europe/Stockholm

Europe/Budapest

Europe/Zagreb

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Paris

Africa/Ndjamena

Africa/Ceuta

Europe/Prague

Europe/Copenhagen

Europe/Vienna

Europe/Tirane

MET

Europe/Amsterdam

Africa/Libreville

Africa/El_Aaiun

Europe/San_Marino

Africa/Douala

Africa/Brazzaville

Africa/Porto-Novo

Poland

Europe/Andorra

Europe/Oslo

Europe/Podgorica

Africa/Casablanca

Africa/Luanda

Atlantic/Jan_Mayen

Africa/Kinshasa

Europe/Madrid

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Bangui

Europe/Belgrade

Africa/Niamey

Europe/Bratislava

Arctic/Longyearbyen

Europe/Vatican

Europe/Monaco

Europe/London

GMT

Etc/GMT-0

Europe/Jersey

Atlantic/St_Helena

Europe/Guernsey

Europe/Isle_of_Man

Etc/GMT+0

Africa/Banjul

Etc/GMT

Africa/Freetown

GB-Eire

Africa/Bamako

GB

Africa/Conakry

Portugal

Universal

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Sao_Tome

Africa/Nouakchott

Antarctica/Troll

UTC

Etc/Universal

Atlantic/Faeroe

Africa/Abidjan

Eire

Africa/Accra

Atlantic/Faroe

Etc/UCT

GMT0

Europe/Dublin

Zulu

Africa/Ouagadougou

Atlantic/Reykjavik

Atlantic/Madeira

Etc/Zulu

Iceland

Europe/Lisbon

Atlantic/Canary

Africa/Lome

Greenwich

Europe/Belfast

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Etc/GMT0

America/Danmarkshavn

Africa/Dakar

Africa/Bissau

WET

Etc/Greenwich

Africa/Timbuktu

UCT

Africa/Monrovia

Etc/UTC

Discover Certificates from IP Range

The API will discover certificates and their private keys from an IP range.

Before you begin

Ensure that the target IP addresses for the network scan are reachable.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values:: ONDEMAND, SCHEDULED
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
description	(Optional) Description of the discovery request. **Type**: String
source	(Mandatory) Network source to discover certificates from **Type**: String **Possible value(s):**: IPRANGE, SUBNET, URL
executeBatchesSequentially	(Optional) Specify if the discovey operation for batches must be executed sequentially **Type**: Boolean **Possible value(s):**: true, false
coolingPeriod	(Mandatory) Indicates whether the discovery is sequential or parallel. **Type**: Integer **Possible value(s):**: • 0 (for parallel discovery) • 1 < (for sequential discovery) **Note:** 1 is not a valid value for this parameter.
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String **Constraint**: Rule name which is added already need to be specified.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
certStatus	(Mandatory) Specify the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: MANAGED, MONITERED, NONE (the values are case sensitive) If **certStatus** = **NONE**, the discovered certificates will not be moved to certificate inventory.
rbacRuleProcessRequired	(Optional) Specify whether RBAC rule process is required. **Type**: Boolean (true or false) **Constraint**: If this is set to **true**, new certificates will be tagged under the group specified in the rule.
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: String
category	(Mandatory) Certificate category **Type**: String **Possible values:**: server, client, code-signing
ipRanges	(Mandatory) Details of the network IP range to be scanned **Type**: ipRanges
occuranceType	(Mandatory) Occurrence frequency **Type**: String **Possible values:**: DAILY, WEEKLY, MONTHLY, YEARLY
neverEnds	(Mandatory) Specify if the discovery should be a never ending occurrence **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible value(s):: true, false
startDate	(Mandatory if **discoveryType** = **SCHEDULED**) Start date for the scheduled network discovery scan **Type**: Long
timeZone	(Mandatory if **discoveryType** = **SCHEDULED**) Time zone in which the scheduled network discovery scan will be triggered **Type**: String **Possible values:**: Possible values for time zone

Payload-ipRanges

Name	Description
startIp	(Mandatory) Starting IP address of the IP range to be scanned for certificate discovery **Type**: String
endIp	(Mandatory) Ending IP address of the IP range to be scanned for certificate discovery **Type**: String
ports	(Mandatory) Target ports to scan **Type**: String **Possible value(s):**: all, comma-separated list of individual ports to be scanned
batchSeperationConstant	(Mandatory) Numerical constant **Type**: String **Possible value(s):**: 0-256
dataCenter	(Mandatory) Data center where the subnet is located

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload-ipRanges (continued)

Name	Description
	Type: String
hostNames	(Mandatory) SNI hostname to be used while retrieving the certificate **Type**: Array
tlsVersions	(Optional) List of TLS versions to be used while communicating with the IP(s) for certificate retrieval **Type**: Array
standardPorts	(Optional) Specify if only standard ports must be scanned **Type**: Boolean **Possible value(s):**: true, false

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message response	Success message of the action or failure description in case of error. **Type**: String
message	Success message or failure description in case of error. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object
header	HTTP headers associated with the response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found. **Remediation**: Ensure that a valid value is provided for the targetList field in the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1. **Remediation**: Provide a correct value in the field coolingPeriod.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Sample Request


```
{
  "discoveryType": "SCHEDULED",
  "name": "IPRange_Disc_ipr1234",
  "description": "",
  "source": "IPRANGE",
  "executeBatchesSequentially": false,
  "coolingPeriod": 0,
  "associatedRule": "",
  "certStatus": "NONE",
  "rbacRuleProcessRequired": false,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"groupName": "Default",
"category": "server",
"ipRanges": [
 {
   "startIp": "192.168.41.0",
   "endIp": "192.168.41.255",
   "ports": "443,8443",
   "batchSeperationConstant": "256",
   "dataCenter": "absecon",
   "hostNames": [],
   "tlsVersions": [
     "TLSv1.2"
   ],
   "standardPorts": false
 },
 {
   "startIp": "192.168.42.0",
   "endIp": "192.168.42.255",
   "ports": "21555",
   "batchSeperationConstant": "100",
   "dataCenter": "absecon",
   "hostNames": [],
   "tlsVersions": [
     "TLSv1.3",
     "TLSv1.2",
     "TLSv1.1",
     "SSLv3"
   ],
   "standardPorts": true
 },
 {
   "startIp": "192.168.43.0",
   "endIp": "192.168.43.255",
   "ports": "all",
   "batchSeperationConstant": "200",
   "dataCenter": "absecon",
   "hostNames": [],
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "tlsVersions": [
      "TLSv1.3",
      "TLSv1.2",
      "TLSv1.1",
      "SSLv3"
    ],
    "standardPorts": false
  }
 ],
 "occuranceType":"MONTHLY",
 "neverEnds" : true,
 "startDate" : 1737636860000,
 "timeZone" : "Pacific/Midway"
}
```


Sample Response


```
{
   "response": {
      "discoveryName": "IPRange_Disc_ipr1234",
      "message": "Discovery scheduler details added successfully with discovery id 67added2c4a3610e43e040b4"
   },
   "message": "Discovery scheduler details added successfully with discovery id 67added2c4a3610e43e040b4",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Possible time zone values

Etc/GMT+12

Pacific/Pago_Pago

Pacific/Samoa

Pacific/Niue

US/Samoa

Etc/GMT+11

Pacific/Midway

Pacific/Honolulu

Pacific/Rarotonga

Pacific/Tahiti

Pacific/Johnston

America/Atka

US/Hawaii

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

SystemV/HST10

America/Adak

US/Aleutian

Etc/GMT+10

Pacific/Marquesas

Etc/GMT+9

US/Alaska

America/Juneau

America/Metlakatla

Pacific/Gambier

America/Yakutat

America/Sitka

SystemV/YST9

America/Anchorage

America/Nome

SystemV/YST9YDT

Etc/GMT+8

Canada/Pacific

PST8PDT

Pacific/Pitcairn

Mexico/BajaNorte

America/Tijuana

SystemV/PST8

America/Santa_Isabel

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Vancouver

America/Ensenada

SystemV/PST8PDT

America/Los_Angeles

US/Pacific

Canada/Yukon

Etc/GMT+7

US/Arizona

Mexico/BajaSur

America/Dawson_Creek

America/Denver

America/Yellowknife

America/Inuvik

America/Ciudad_Juarez

America/Mazatlan

SystemV/MST7

America/Boise

America/Dawson

MST7MDT

US/Mountain

America/Creston

America/Edmonton

America/Hermosillo

Canada/Mountain

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Cambridge_Bay

Navajo

America/Phoenix

America/Whitehorse

SystemV/MST7MDT

America/Fort_Nelson

America/Shiprock

America/El_Salvador

America/Guatemala

America/Belize

America/Managua

America/Chicago

America/Tegucigalpa

Etc/GMT+6

America/Regina

Mexico/General

America/Rankin_Inlet

US/Central

Pacific/Galapagos

America/Rainy_River

America/Swift_Current

America/Costa_Rica

America/Indiana/Knox

America/North_Dakota/Beulah

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Monterrey

SystemV/CST6

America/North_Dakota/Center

America/Indiana/Tell_City

America/Chihuahua

America/Ojinaga

America/Mexico_City

America/Matamoros

CST6CDT

America/Knox_IN

America/Menominee

America/Resolute

Canada/Central

America/Bahia_Banderas

US/Indiana-Starke

SystemV/CST6CDT

America/Merida

Canada/Saskatchewan

America/North_Dakota/New_Salem

America/Winnipeg

America/Panama

America/Indiana/Petersburg

America/Eirunepe

America/Grand_Turk

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Cuba

Etc/GMT+5

Pacific/Easter

America/Fort_Wayne

America/Havana

America/Porto_Acre

US/Michigan

America/Louisville

America/Guayaquil

America/Indiana/Vevay

America/Indiana/Vincennes

America/Indianapolis

America/Iqaluit

America/Kentucky/Louisville

EST5EDT

America/Nassau

America/Jamaica

America/Atikokan

America/Kentucky/Monticello

America/Coral_Harbour

America/Cayman

Chile/EasterIsland

America/Indiana/Indianapolis

America/Thunder_Bay

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Indiana/Marengo

America/Bogota

SystemV/EST5

US/Eastern

Canada/Eastern

America/Port-au-Prince

America/Nipigon

Brazil/Acre

US/East-Indiana

America/Cancun

America/Lima

America/Rio_Branco

America/Detroit

Jamaica

America/Pangnirtung

America/Montreal

America/Indiana/Winamac

America/New_York

America/Toronto

SystemV/EST5EDT

America/Cuiaba

America/Marigot

Canada/Atlantic

Etc/GMT+4

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Manaus

America/St_Thomas

America/Anguilla

America/Barbados

America/Curacao

America/Guyana

America/Martinique

America/Puerto_Rico

America/Port_of_Spain

SystemV/AST4

America/Kralendijk

America/Antigua

America/Moncton

America/St_Vincent

America/Dominica

Atlantic/Bermuda

Brazil/West

America/Aruba

America/Halifax

America/La_Paz

America/Blanc-Sablon

America/Santo_Domingo

America/Glace_Bay

America/St_Barthelemy

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/St_Lucia

America/Montserrat

America/Lower_Princes

America/Thule

America/Tortola

America/Porto_Velho

America/Campo_Grande

America/Goose_Bay

America/Virgin

America/Boa_Vista

America/Grenada

America/St_Kitts

America/Caracas

America/Guadeloupe

SystemV/AST4ADT

America/St_Johns

Canada/Newfoundland

Chile/Continental

America/Miquelon

America/Argentina/Catamarca

America/Argentina/Cordoba

America/Araguaina

America/Argentina/Salta

Etc/GMT+3

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Montevideo

Brazil/East

America/Argentina/Mendoza

America/Argentina/Rio_Gallegos

America/Catamarca

America/Cordoba

America/Sao_Paulo

America/Argentina/Jujuy

America/Cayenne

America/Recife

America/Buenos_Aires

America/Paramaribo

America/Mendoza

America/Santarem

America/Asuncion

America/Maceio

Atlantic/Stanley

Antarctica/Rothera

America/Argentina/San_Luis

America/Santiago

America/Argentina/Ushuaia

Antarctica/Palmer

America/Punta_Arenas

America/Fortaleza

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Argentina/La_Rioja

America/Belem

America/Jujuy

America/Bahia

America/Argentina/San_Juan

America/Argentina/ComodRivadavia

America/Argentina/Tucuman

America/Rosario

America/Argentina/Buenos_Aires

Etc/GMT+2

America/Godthab

America/Noronha

Brazil/DeNoronha

Atlantic/South_Georgia

America/Scoresbysund

America/Nuuk

Etc/GMT+1

Atlantic/Cape_Verde

Atlantic/Azores

Pacific/Kiritimati

Etc/GMT-14

NZ-CHAT

Pacific/Chatham

Pacific/Fakaofo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Antarctica/McMurdo

Pacific/Enderbury

NZ

Pacific/Apia

Antarctica/South_Pole

Pacific/Kanton

Pacific/Auckland

Pacific/Tongatapu

Etc/GMT-13

Pacific/Kwajalein

Pacific/Wallis

Pacific/Fiji

Pacific/Funafuti

Pacific/Nauru

Kwajalein

Pacific/Wake

Pacific/Norfolk

Pacific/Tarawa

Asia/Kamchatka

Etc/GMT-12

Asia/Anadyr

Pacific/Majuro

Australia/Hobart

Australia/Tasmania

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/ACT

Pacific/Ponape

Pacific/Bougainville

Australia/Victoria

Antarctica/Macquarie

Australia/Canberra

Australia/Currie

Australia/Lord_Howe

Australia/NSW

Pacific/Pohnpei

Pacific/Efate

Asia/Magadan

Pacific/Kosrae

Australia/Sydney

Australia/LHI

Asia/Sakhalin

Pacific/Noumea

Etc/GMT-11

Asia/Srednekolymsk

Australia/Melbourne

Pacific/Guadalcanal

Australia/Yancowinna

Australia/Adelaide

Australia/Broken_Hill

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/South

Pacific/Yap

Pacific/Port_Moresby

Pacific/Chuuk

Australia/Queensland

Pacific/Guam

Pacific/Truk

Asia/Vladivostok

Pacific/Saipan

Antarctica/DumontDUrville

Australia/Brisbane

Etc/GMT-10

Asia/Ust-Nera

Australia/Lindeman

Australia/North

Australia/Darwin

Etc/GMT-9

Pacific/Palau

Asia/Chita

Asia/Dili

Asia/Jayapura

Asia/Yakutsk

Asia/Pyongyang

ROK

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Seoul

Asia/Khandyga

Japan

Asia/Tokyo

Australia/Eucla

Asia/Kuching

Asia/Chungking

Etc/GMT-8

Australia/Perth

Asia/Macao

Asia/Macau

Asia/Choibalsan

Asia/Shanghai

Antarctica/Casey

Asia/Ulan_Bator

Asia/Chongqing

Asia/Ulaanbaatar

Asia/Taipei

Asia/Manila

PRC

Asia/Ujung_Pandang

Asia/Harbin

Singapore

Asia/Brunei

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/West

Asia/Hong_Kong

Asia/Makassar

Hongkong

Asia/Kuala_Lumpur

Asia/Irkutsk

Asia/Singapore

Asia/Pontianak

Etc/GMT-7

Asia/Phnom_Penh

Asia/Novosibirsk

Antarctica/Davis

Asia/Tomsk

Asia/Jakarta

Asia/Barnaul

Indian/Christmas

Asia/Ho_Chi_Minh

Asia/Hovd

Asia/Bangkok

Asia/Vientiane

Asia/Novokuznetsk

Asia/Krasnoyarsk

Asia/Saigon

Asia/Yangon

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Rangoon

Indian/Cocos

Asia/Kashgar

Etc/GMT-6

Asia/Dacca

Asia/Omsk

Asia/Dhaka

Indian/Chagos

Asia/Bishkek

Asia/Urumqi

Asia/Thimbu

Asia/Thimphu

Asia/Kathmandu

Asia/Katmandu

Asia/Kolkata

Asia/Colombo

Asia/Calcutta

Asia/Aqtau

Etc/GMT-5

Asia/Samarkand

Asia/Almaty

Asia/Karachi

Asia/Yekaterinburg

Asia/Dushanbe

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Indian/Maldives

Asia/Oral

Asia/Tashkent

Asia/Qostanay

Antarctica/Mawson

Asia/Qyzylorda

Asia/Aqtobe

Asia/Ashkhabad

Antarctica/Vostok

Asia/Ashgabat

Asia/Atyrau

Indian/Kerguelen

Asia/Kabul

Asia/Yerevan

Etc/GMT-4

Asia/Dubai

Indian/Reunion

Indian/Mauritius

Europe/Saratov

Europe/Samara

Indian/Mahe

Asia/Baku

Asia/Muscat

Europe/Astrakhan

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Tbilisi

Europe/Ulyanovsk

Iran

Asia/Tehran

Asia/Aden

Africa/Nairobi

Europe/Istanbul

Etc/GMT-3

Indian/Comoro

Antarctica/Syowa

Africa/Mogadishu

Africa/Asmera

Asia/Istanbul

Europe/Moscow

Africa/Djibouti

Europe/Simferopol

Africa/Asmara

Asia/Baghdad

Asia/Damascus

Africa/Dar_es_Salaam

Africa/Addis_Ababa

Asia/Riyadh

Asia/Kuwait

Europe/Kirov

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Kampala

Europe/Minsk

Asia/Qatar

Asia/Bahrain

Indian/Antananarivo

Indian/Mayotte

Europe/Volgograd

Turkey

W-SU

Asia/Amman

Africa/Cairo

Africa/Mbabane

Etc/GMT-2

Europe/Zaporozhye

Libya

Africa/Kigali

Africa/Tripoli

Israel

Europe/Kaliningrad

Africa/Windhoek

Europe/Bucharest

Europe/Mariehamn

Africa/Lubumbashi

Europe/Tiraspol

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Chisinau

Europe/Helsinki

Asia/Beirut

Asia/Tel_Aviv

Europe/Sofia

Africa/Gaborone

Asia/Gaza

Europe/Riga

Africa/Maputo

Europe/Uzhgorod

Asia/Jerusalem

Africa/Bujumbura

Europe/Kiev

Europe/Vilnius

Africa/Maseru

Africa/Blantyre

Africa/Lusaka

Africa/Harare

Europe/Tallinn

Africa/Khartoum

Africa/Johannesburg

Africa/Juba

Europe/Kyiv

Asia/Nicosia

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Famagusta

EET

Asia/Hebron

Egypt

Europe/Nicosia

Europe/Athens

Europe/Brussels

Europe/Warsaw

CET

Etc/GMT-1

Europe/Luxembourg

Africa/Tunis

Europe/Malta

Europe/Busingen

Africa/Malabo

Europe/Skopje

Europe/Sarajevo

Africa/Lagos

Europe/Rome

Africa/Algiers

Europe/Zurich

Europe/Gibraltar

Europe/Vaduz

Europe/Ljubljana

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Berlin

Europe/Stockholm

Europe/Budapest

Europe/Zagreb

Europe/Paris

Africa/Ndjamena

Africa/Ceuta

Europe/Prague

Europe/Copenhagen

Europe/Vienna

Europe/Tirane

MET

Europe/Amsterdam

Africa/Libreville

Africa/El_Aaiun

Europe/San_Marino

Africa/Douala

Africa/Brazzaville

Africa/Porto-Novo

Poland

Europe/Andorra

Europe/Oslo

Europe/Podgorica

Africa/Casablanca

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Luanda

Atlantic/Jan_Mayen

Africa/Kinshasa

Europe/Madrid

Africa/Bangui

Europe/Belgrade

Africa/Niamey

Europe/Bratislava

Arctic/Longyearbyen

Europe/Vatican

Europe/Monaco

Europe/London

GMT

Etc/GMT-0

Europe/Jersey

Atlantic/St_Helena

Europe/Guernsey

Europe/Isle_of_Man

Etc/GMT+0

Africa/Banjul

Etc/GMT

Africa/Freetown

GB-Eire

Africa/Bamako

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

GB

Africa/Conakry

Portugal

Universal

Africa/Sao_Tome

Africa/Nouakchott

Antarctica/Troll

UTC

Etc/Universal

Atlantic/Faeroe

Africa/Abidjan

Eire

Africa/Accra

Atlantic/Faroe

Etc/UCT

GMT0

Europe/Dublin

Zulu

Africa/Ouagadougou

Atlantic/Reykjavik

Atlantic/Madeira

Etc/Zulu

Iceland

Europe/Lisbon

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Atlantic/Canary

Africa/Lome

Greenwich

Europe/Belfast

Etc/GMT0

America/Danmarkshavn

Africa/Dakar

Africa/Bissau

WET

Etc/Greenwich

Africa/Timbuktu

UCT

Africa/Monrovia

Etc/UTC

Discover Certificates from URL

The API will discover certificates and their private keys from an HTTPS URL.

Before you begin

Ensure that the target IP addresses for the network scan are reachable.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?gwsource=external

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To understand the elements of the sample URL, click here.
Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String **Possible values:**: ONDEMAND, SCHEDULED
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
description	(Optional) Description of the discovery request. **Type**: String
source	(Mandatory) Network source to discover certificates from **Type**: String **Possible value(s):**: IPRANGE, SUBNET, URL
executeBatchesSequentially	(Optional) Specify if the discovey operation for batches must be executed sequentially **Type**: Boolean **Possible value(s):**: true, false
coolingPeriod	(Mandatory) Indicates whether the discovery is sequential or parallel. **Type**: Integer **Possible value(s):**: • 0 (for parallel discovery) • 1 < (for sequential discovery) **Note:** 1 is not a valid value for this parameter.
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraint**: Rule name which is added already need to be specified.
certStatus	(Mandatory) Specify the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: MANAGED, MONITERED, NONE (the values are case sensitive) If **certStatus** = **NONE**, the discovered certificates will not be moved to certificate inventory.
rbacRuleProcessRequired	(Optional) Specify whether RBAC rule process is required. **Type**: Boolean (true or false) **Constraint**: If this is set to **true**, new certificates will be tagged under the group specified in the rule.
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: String
category	(Mandatory) Certificate category **Type**: String **Possible values:**: server, client, code-signing
urls	(Mandatory) Details of the HTTPS URL to be scanned **Type**: urls
occuranceType	(Mandatory) Occurrence frequency **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values:: DAILY, WEEKLY, MONTHLY, YEARLY
neverEnds	(Mandatory) Specify if the discovery should be a never ending occurrence **Type**: Boolean **Possible value(s):**: true, false
startDate	(Mandatory if **discoveryType** = **SCHEDULED**) Start date for the scheduled network discovery scan **Type**: Long
timeZone	(Mandatory if **discoveryType** = **SCHEDULED**) Time zone in which the scheduled network discovery scan will be triggered **Type**: String **Possible values:**: Possible values for time zone

Payload-urls

Name	Description
url	(Mandatory) HTTPS URL to be scanned for certificate discovery **Type**: String
ports	(Mandatory) Target ports to scan **Type**: String **Possible value(s):**: all, comma-separated list of individual ports to be scanned
dataCenter	(Mandatory) Data center where the subnet is located **Type**: String
hostNames	(Mandatory) SNI hostname to be used while retrieving the certificate **Type**: Array

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload-urls (continued)

Name	Description
tlsVersions	(Optional) List of TLS versions to be used while communicating with the IP(s) for certificate retrieval **Type**: Array

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message response	Success message of the action or failure description in case of error. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object
header	HTTP headers associated with the response. **Type**: Object

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found. **Remediation**: Ensure that a valid value is provided for the targetList field in the request.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Provide a correct value in the field coolingPeriod.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Sample Request


```
{
 "discoveryType": "SCHEDULED",
 "name": "Subnet_Disc_URL",
 "description": "",
 "source": "URL",
 "executeBatchesSequentially": false,
 "coolingPeriod": 0,
 "associatedRule": "",
 "certStatus": "NONE",
 "rbacRuleProcessRequired": false,
 "groupName": "Default",
 "category": "server",
 "urls": [
  {
   "url": "google.com",
   "ports": "443,8443",
   "dataCenter": "absecon",
   "hostNames": ["google.com"],
   "tlsVersions": ["TLSv1.2"]
  },
  {
   "url": "yahoo.com",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "ports": "all",
    "dataCenter": "absecon",
    "hostNames": [],
    "tlsVersions": ["TLSv1.2", "TLSv1.3"]
   }
 ],
 "occuranceType":"YEARLY",
 "neverEnds" : true,
 "startDate" : 1737636860000,
 "timeZone" : "Europe/Istanbul"
}
```


Sample Response


```
{
   "response": {
      "discoveryName": "Subnet_Disc_URL",
      "message": "Discovery scheduler details added successfully with discovery id 67added2c4a3610e43e040b4"
   },
   "message": "Discovery scheduler details added successfully with discovery id 67added2c4a3610e43e040b4",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Possible time zone values

Etc/GMT+12

Pacific/Pago_Pago

Pacific/Samoa

Pacific/Niue

US/Samoa

Etc/GMT+11

Pacific/Midway

Pacific/Honolulu

Pacific/Rarotonga

Pacific/Tahiti

Pacific/Johnston

America/Atka

US/Hawaii

SystemV/HST10

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Adak

US/Aleutian

Etc/GMT+10

Pacific/Marquesas

Etc/GMT+9

US/Alaska

America/Juneau

America/Metlakatla

Pacific/Gambier

America/Yakutat

America/Sitka

SystemV/YST9

America/Anchorage

America/Nome

SystemV/YST9YDT

Etc/GMT+8

Canada/Pacific

PST8PDT

Pacific/Pitcairn

Mexico/BajaNorte

America/Tijuana

SystemV/PST8

America/Santa_Isabel

America/Vancouver

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Ensenada

SystemV/PST8PDT

America/Los_Angeles

US/Pacific

Canada/Yukon

Etc/GMT+7

US/Arizona

Mexico/BajaSur

America/Dawson_Creek

America/Denver

America/Yellowknife

America/Inuvik

America/Ciudad_Juarez

America/Mazatlan

SystemV/MST7

America/Boise

America/Dawson

MST7MDT

US/Mountain

America/Creston

America/Edmonton

America/Hermosillo

Canada/Mountain

America/Cambridge_Bay

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Navajo

America/Phoenix

America/Whitehorse

SystemV/MST7MDT

America/Fort_Nelson

America/Shiprock

America/El_Salvador

America/Guatemala

America/Belize

America/Managua

America/Chicago

America/Tegucigalpa

Etc/GMT+6

America/Regina

Mexico/General

America/Rankin_Inlet

US/Central

Pacific/Galapagos

America/Rainy_River

America/Swift_Current

America/Costa_Rica

America/Indiana/Knox

America/North_Dakota/Beulah

America/Monterrey

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

SystemV/CST6

America/North_Dakota/Center

America/Indiana/Tell_City

America/Chihuahua

America/Ojinaga

America/Mexico_City

America/Matamoros

CST6CDT

America/Knox_IN

America/Menominee

America/Resolute

Canada/Central

America/Bahia_Banderas

US/Indiana-Starke

SystemV/CST6CDT

America/Merida

Canada/Saskatchewan

America/North_Dakota/New_Salem

America/Winnipeg

America/Panama

America/Indiana/Petersburg

America/Eirunepe

America/Grand_Turk

Cuba

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Etc/GMT+5

Pacific/Easter

America/Fort_Wayne

America/Havana

America/Porto_Acre

US/Michigan

America/Louisville

America/Guayaquil

America/Indiana/Vevay

America/Indiana/Vincennes

America/Indianapolis

America/Iqaluit

America/Kentucky/Louisville

EST5EDT

America/Nassau

America/Jamaica

America/Atikokan

America/Kentucky/Monticello

America/Coral_Harbour

America/Cayman

Chile/EasterIsland

America/Indiana/Indianapolis

America/Thunder_Bay

America/Indiana/Marengo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Bogota

SystemV/EST5

US/Eastern

Canada/Eastern

America/Port-au-Prince

America/Nipigon

Brazil/Acre

US/East-Indiana

America/Cancun

America/Lima

America/Rio_Branco

America/Detroit

Jamaica

America/Pangnirtung

America/Montreal

America/Indiana/Winamac

America/New_York

America/Toronto

SystemV/EST5EDT

America/Cuiaba

America/Marigot

Canada/Atlantic

Etc/GMT+4

America/Manaus

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/St_Thomas

America/Anguilla

America/Barbados

America/Curacao

America/Guyana

America/Martinique

America/Puerto_Rico

America/Port_of_Spain

SystemV/AST4

America/Kralendijk

America/Antigua

America/Moncton

America/St_Vincent

America/Dominica

Atlantic/Bermuda

Brazil/West

America/Aruba

America/Halifax

America/La_Paz

America/Blanc-Sablon

America/Santo_Domingo

America/Glace_Bay

America/St_Barthelemy

America/St_Lucia

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Montserrat

America/Lower_Princes

America/Thule

America/Tortola

America/Porto_Velho

America/Campo_Grande

America/Goose_Bay

America/Virgin

America/Boa_Vista

America/Grenada

America/St_Kitts

America/Caracas

America/Guadeloupe

SystemV/AST4ADT

America/St_Johns

Canada/Newfoundland

Chile/Continental

America/Miquelon

America/Argentina/Catamarca

America/Argentina/Cordoba

America/Araguaina

America/Argentina/Salta

Etc/GMT+3

America/Montevideo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Brazil/East

America/Argentina/Mendoza

America/Argentina/Rio_Gallegos

America/Catamarca

America/Cordoba

America/Sao_Paulo

America/Argentina/Jujuy

America/Cayenne

America/Recife

America/Buenos_Aires

America/Paramaribo

America/Mendoza

America/Santarem

America/Asuncion

America/Maceio

Atlantic/Stanley

Antarctica/Rothera

America/Argentina/San_Luis

America/Santiago

America/Argentina/Ushuaia

Antarctica/Palmer

America/Punta_Arenas

America/Fortaleza

America/Argentina/La_Rioja

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Belem

America/Jujuy

America/Bahia

America/Argentina/San_Juan

America/Argentina/ComodRivadavia

America/Argentina/Tucuman

America/Rosario

America/Argentina/Buenos_Aires

Etc/GMT+2

America/Godthab

America/Noronha

Brazil/DeNoronha

Atlantic/South_Georgia

America/Scoresbysund

America/Nuuk

Etc/GMT+1

Atlantic/Cape_Verde

Atlantic/Azores

Pacific/Kiritimati

Etc/GMT-14

NZ-CHAT

Pacific/Chatham

Pacific/Fakaofo

Antarctica/McMurdo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Enderbury

NZ

Pacific/Apia

Antarctica/South_Pole

Pacific/Kanton

Pacific/Auckland

Pacific/Tongatapu

Etc/GMT-13

Pacific/Kwajalein

Pacific/Wallis

Pacific/Fiji

Pacific/Funafuti

Pacific/Nauru

Kwajalein

Pacific/Wake

Pacific/Norfolk

Pacific/Tarawa

Asia/Kamchatka

Etc/GMT-12

Asia/Anadyr

Pacific/Majuro

Australia/Hobart

Australia/Tasmania

Australia/ACT

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Ponape

Pacific/Bougainville

Australia/Victoria

Antarctica/Macquarie

Australia/Canberra

Australia/Currie

Australia/Lord_Howe

Australia/NSW

Pacific/Pohnpei

Pacific/Efate

Asia/Magadan

Pacific/Kosrae

Australia/Sydney

Australia/LHI

Asia/Sakhalin

Pacific/Noumea

Etc/GMT-11

Asia/Srednekolymsk

Australia/Melbourne

Pacific/Guadalcanal

Australia/Yancowinna

Australia/Adelaide

Australia/Broken_Hill

Australia/South

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Yap

Pacific/Port_Moresby

Pacific/Chuuk

Australia/Queensland

Pacific/Guam

Pacific/Truk

Asia/Vladivostok

Pacific/Saipan

Antarctica/DumontDUrville

Australia/Brisbane

Etc/GMT-10

Asia/Ust-Nera

Australia/Lindeman

Australia/North

Australia/Darwin

Etc/GMT-9

Pacific/Palau

Asia/Chita

Asia/Dili

Asia/Jayapura

Asia/Yakutsk

Asia/Pyongyang

ROK

Asia/Seoul

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Khandyga

Japan

Asia/Tokyo

Australia/Eucla

Asia/Kuching

Asia/Chungking

Etc/GMT-8

Australia/Perth

Asia/Macao

Asia/Macau

Asia/Choibalsan

Asia/Shanghai

Antarctica/Casey

Asia/Ulan_Bator

Asia/Chongqing

Asia/Ulaanbaatar

Asia/Taipei

Asia/Manila

PRC

Asia/Ujung_Pandang

Asia/Harbin

Singapore

Asia/Brunei

Australia/West

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Hong_Kong

Asia/Makassar

Hongkong

Asia/Kuala_Lumpur

Asia/Irkutsk

Asia/Singapore

Asia/Pontianak

Etc/GMT-7

Asia/Phnom_Penh

Asia/Novosibirsk

Antarctica/Davis

Asia/Tomsk

Asia/Jakarta

Asia/Barnaul

Indian/Christmas

Asia/Ho_Chi_Minh

Asia/Hovd

Asia/Bangkok

Asia/Vientiane

Asia/Novokuznetsk

Asia/Krasnoyarsk

Asia/Saigon

Asia/Yangon

Asia/Rangoon

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Indian/Cocos

Asia/Kashgar

Etc/GMT-6

Asia/Dacca

Asia/Omsk

Asia/Dhaka

Indian/Chagos

Asia/Bishkek

Asia/Urumqi

Asia/Thimbu

Asia/Thimphu

Asia/Kathmandu

Asia/Katmandu

Asia/Kolkata

Asia/Colombo

Asia/Calcutta

Asia/Aqtau

Etc/GMT-5

Asia/Samarkand

Asia/Almaty

Asia/Karachi

Asia/Yekaterinburg

Asia/Dushanbe

Indian/Maldives

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Oral

Asia/Tashkent

Asia/Qostanay

Antarctica/Mawson

Asia/Qyzylorda

Asia/Aqtobe

Asia/Ashkhabad

Antarctica/Vostok

Asia/Ashgabat

Asia/Atyrau

Indian/Kerguelen

Asia/Kabul

Asia/Yerevan

Etc/GMT-4

Asia/Dubai

Indian/Reunion

Indian/Mauritius

Europe/Saratov

Europe/Samara

Indian/Mahe

Asia/Baku

Asia/Muscat

Europe/Astrakhan

Asia/Tbilisi

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Ulyanovsk

Iran

Asia/Tehran

Asia/Aden

Africa/Nairobi

Europe/Istanbul

Etc/GMT-3

Indian/Comoro

Antarctica/Syowa

Africa/Mogadishu

Africa/Asmera

Asia/Istanbul

Europe/Moscow

Africa/Djibouti

Europe/Simferopol

Africa/Asmara

Asia/Baghdad

Asia/Damascus

Africa/Dar_es_Salaam

Africa/Addis_Ababa

Asia/Riyadh

Asia/Kuwait

Europe/Kirov

Africa/Kampala

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Minsk

Asia/Qatar

Asia/Bahrain

Indian/Antananarivo

Indian/Mayotte

Europe/Volgograd

Turkey

W-SU

Asia/Amman

Africa/Cairo

Africa/Mbabane

Etc/GMT-2

Europe/Zaporozhye

Libya

Africa/Kigali

Africa/Tripoli

Israel

Europe/Kaliningrad

Africa/Windhoek

Europe/Bucharest

Europe/Mariehamn

Africa/Lubumbashi

Europe/Tiraspol

Europe/Chisinau

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Helsinki

Asia/Beirut

Asia/Tel_Aviv

Europe/Sofia

Africa/Gaborone

Asia/Gaza

Europe/Riga

Africa/Maputo

Europe/Uzhgorod

Asia/Jerusalem

Africa/Bujumbura

Europe/Kiev

Europe/Vilnius

Africa/Maseru

Africa/Blantyre

Africa/Lusaka

Africa/Harare

Europe/Tallinn

Africa/Khartoum

Africa/Johannesburg

Africa/Juba

Europe/Kyiv

Asia/Nicosia

Asia/Famagusta

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

EET

Asia/Hebron

Egypt

Europe/Nicosia

Europe/Athens

Europe/Brussels

Europe/Warsaw

CET

Etc/GMT-1

Europe/Luxembourg

Africa/Tunis

Europe/Malta

Europe/Busingen

Africa/Malabo

Europe/Skopje

Europe/Sarajevo

Africa/Lagos

Europe/Rome

Africa/Algiers

Europe/Zurich

Europe/Gibraltar

Europe/Vaduz

Europe/Ljubljana

Europe/Berlin

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Stockholm

Europe/Budapest

Europe/Zagreb

Europe/Paris

Africa/Ndjamena

Africa/Ceuta

Europe/Prague

Europe/Copenhagen

Europe/Vienna

Europe/Tirane

MET

Europe/Amsterdam

Africa/Libreville

Africa/El_Aaiun

Europe/San_Marino

Africa/Douala

Africa/Brazzaville

Africa/Porto-Novo

Poland

Europe/Andorra

Europe/Oslo

Europe/Podgorica

Africa/Casablanca

Africa/Luanda

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Atlantic/Jan_Mayen

Africa/Kinshasa

Europe/Madrid

Africa/Bangui

Europe/Belgrade

Africa/Niamey

Europe/Bratislava

Arctic/Longyearbyen

Europe/Vatican

Europe/Monaco

Europe/London

GMT

Etc/GMT-0

Europe/Jersey

Atlantic/St_Helena

Europe/Guernsey

Europe/Isle_of_Man

Etc/GMT+0

Africa/Banjul

Etc/GMT

Africa/Freetown

GB-Eire

Africa/Bamako

GB

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Conakry

Portugal

Universal

Africa/Sao_Tome

Africa/Nouakchott

Antarctica/Troll

UTC

Etc/Universal

Atlantic/Faeroe

Africa/Abidjan

Eire

Africa/Accra

Atlantic/Faroe

Etc/UCT

GMT0

Europe/Dublin

Zulu

Africa/Ouagadougou

Atlantic/Reykjavik

Atlantic/Madeira

Etc/Zulu

Iceland

Europe/Lisbon

Atlantic/Canary

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Lome

Greenwich

Europe/Belfast

Etc/GMT0

America/Danmarkshavn

Africa/Dakar

Africa/Bissau

WET

Etc/Greenwich

Africa/Timbuktu

UCT

Africa/Monrovia

Etc/UTC

Discover Certificates from Network

The API will discover certificates and their private keys from a network.

Before you begin

Ensure that the provided networks are valid.

Request Structure

Endpoint:	/certificate/discovery/instance
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?gwsource=external` To understand the elements of the sample URL, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Headers
Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
discoveryType	(Mandatory) Type of the discovery. **Type**: String **Possible values:**: ONDEMAND
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
description	(Optional) Description of the discovery request. **Type**: String
source	(Mandatory) Network source to discover certificates from **Type**: String **Important**: The values are case-sensitive. **Possible value(s):**: IPRANGE, SUBNET, URL
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String **Possible value(s):**: Rule name which is added already need to be specified.
certStatus	(Mandatory) Specify the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible value(s)**: MANAGED, MONITORED, or NONE. If "None", then certificates will not be moved to certificate inventory.
associatedRule	(Optional) Name of the rule to be associated with the discovered certificates. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Rule name which is added already need to be specified.
certStatus	(Mandatory) Specify the certificate status to be maintained in the inventory after discovering the certificates. **Type**: String **Possible values:**: MANAGED, MONITERED, NONE (the values are case sensitive) **Important**: The values are case-sensitive. If **certStatus** = **NONE**, the discovered certificates will not be moved to certificate inventory.
rbacRuleProcessRequired	(Optional) Specify whether RBAC rule process is required. **Type**: Boolean (true or false) **Constraint**: If this is set to **true**, new certificates will be tagged under the group specified in the rule.
groupName	(Mandatory) Specifies the group under which the discovered certificate needs to be tagged. **Type**: String
networkList	(Mandatory) List of the networks to be scanned. **Type**: String
category	(Mandatory) Certificate category **Type**: String **Possible values:**: server, client, code-signing
occuranceType	(Mandatory) Occurrence frequency **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values:: DAILY, WEEKLY, MONTHLY, YEARLY
neverEnds	(Mandatory) Specify if the discovery should be a never ending occurrence **Type**: Boolean **Possible value(s):**: true, false
startDate	(Mandatory if **discoveryType** = **SCHEDULED**) Start date for the scheduled network discovery scan **Type**: Long
timeZone	(Mandatory if **discoveryType** = **SCHEDULED**) Time zone in which the scheduled network discovery scan will be triggered **Type**: String **Possible values:**: Possible values for time zone
endDate	(Optional - Applicable for discoveryType = SCHEDULED). End date for the scheduled network discovery scan. **Type**: Long
endAfterNoOfOccurances	(Optional - Applicable for discoveryType = SCHEDULED). Number of occurrences after which the scheduled network discovery scan is ended. **Type**: Integer
occuranceDays	(Optional - Applicable for discoveryType = SCHEDULED AND occuranceType = WEEKLY). List of days of week in which the scheduled discovery to be triggered. **Type**: List **Possible Value**: MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY **Default Value**: MONDAY

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
hostNames	(Optional) Comma separated sni host names. **Type**: String
passiveMode	(Optional - Applicable for discoveryType = SCHEDULED). If passiveMode is true; Discover certificates from IPs and ports from which certificates were discovered previously. **Type**: Boolean **Default value**: False
fullScanAfterNumberOfPassiveDiscoveries	(Optional - Applicable for discoveryType = SCHEDULED AND passiveMode = true). The number of passive discoveries after which full scan needs to be run. **Type**: Integer **Default value**: 0

Note: If endAfterNoOfOccurances is null or 0, and endDate is null, and neverEnds is either null or false, then neverEnds will be automatically set to true.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request. **Type**: Object
discoveryName response	Name of the discovery request created. **Type**: String
message	Success message of the action or failure description in case of error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null for failure response. **Type**: String
tags	Additional information in case of a failure response. **Type**: Object
header	HTTP headers associated with the response. **Type**: Object

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Discovery history details added successfully with discovery id<value>, and discovery operation has been triggered.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the <<field name>> field in the request.
400 Bad Request	INVALID_REQUEST	Target list not found. **Remediation**: Ensure that a valid value is provided for the targetList field in the request.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: Provide a different Discovery name.
417 Expectation failed	GROUP_NOT_FOUND	Specified certificate group is not found. **Remediation**: Ensure that valid value is provided for the groupName section in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Cooling period should be 0 or greater than 1. **Remediation**: Provide a correct value in the field coolingPeriod.
417 Expectation failed	FIELD_VALUE_INVALID	Discovery Type should be ONDEMAND or SCHEDULED. **Remediation**: Provide a correct value in the field discoveryType.
500 Internal Server Error	avx-common-011	Error while processing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Sample Request

```
{
    "discoveryType": "ONDEMAND",
    "name": "on_demand_network",
    "description": "on_demand_network desc",
    "source": "NETWORK",
    "groupName": "Default",
    "networkList" : [
"BLR_network"
    ],
    "certStatus": "NONE",
    "rbacRuleProcessRequired" : false,
    "associatedRule": "ignore_revoked_certs"
}
```

Sample Request

```
{
    "discoveryType": "SCHEDULED",
    "name": "scheduled_network",
    "description": "scheduled_network desc",
    "source": "NETWORK",
    "groupName": "Default",
    "networkList" : [
        "BLR_network"
    ],
    "certStatus": "MANAGED",
    "rbacRuleProcessRequired" : false,
    "associatedRule": "ignore_revoked_certs",
    "occuranceType": "WEEKLY",
    "occuranceDays": ["TUESDAY", "WEDNESDAY"],
    "neverEnds": true,
    "startDate": 1749555000000,
    "hostNames": "appviewx.com",
    "passiveMode": false,
    "fullScanAfterNumberOfPassiveDiscoveries": 0,
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "timeZone":"Asia/Calcutta"
}
```

Sample Response

```
{
  "response": {
     "discoveryName": "on_demand_network",
     "message": "Discovery history details added successfully with discovery id 683d53800b80a91c95bee4da, and discovery operation has been triggered."
  },
  "message": "Discovery history details added successfully with discovery id 683d53800b80a91c95bee4da, and discovery operation has been triggered.",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Possible time zone values

Etc/GMT+12

Pacific/Pago_Pago

Pacific/Samoa

Pacific/Niue

US/Samoa

Etc/GMT+11

Pacific/Midway

Pacific/Honolulu

Pacific/Rarotonga

Pacific/Tahiti

Pacific/Johnston

America/Atka

US/Hawaii

SystemV/HST10

America/Adak

US/Aleutian

Etc/GMT+10

Pacific/Marquesas

Etc/GMT+9

US/Alaska

America/Juneau

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Metlakatla

Pacific/Gambier

America/Yakutat

America/Sitka

SystemV/YST9

America/Anchorage

America/Nome

SystemV/YST9YDT

Etc/GMT+8

Canada/Pacific

PST8PDT

Pacific/Pitcairn

Mexico/BajaNorte

America/Tijuana

SystemV/PST8

America/Santa_Isabel

America/Vancouver

America/Ensenada

SystemV/PST8PDT

America/Los_Angeles

US/Pacific

Canada/Yukon

Etc/GMT+7

US/Arizona

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Mexico/BajaSur

America/Dawson_Creek

America/Denver

America/Yellowknife

America/Inuvik

America/Ciudad_Juarez

America/Mazatlan

SystemV/MST7

America/Boise

America/Dawson

MST7MDT

US/Mountain

America/Creston

America/Edmonton

America/Hermosillo

Canada/Mountain

America/Cambridge_Bay

Navajo

America/Phoenix

America/Whitehorse

SystemV/MST7MDT

America/Fort_Nelson

America/Shiprock

America/El_Salvador

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Guatemala

America/Belize

America/Managua

America/Chicago

America/Tegucigalpa

Etc/GMT+6

America/Regina

Mexico/General

America/Rankin_Inlet

US/Central

Pacific/Galapagos

America/Rainy_River

America/Swift_Current

America/Costa_Rica

America/Indiana/Knox

America/North_Dakota/Beulah

America/Monterrey

SystemV/CST6

America/North_Dakota/Center

America/Indiana/Tell_City

America/Chihuahua

America/Ojinaga

America/Mexico_City

America/Matamoros

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CST6CDT

America/Knox_IN

America/Menominee

America/Resolute

Canada/Central

America/Bahia_Banderas

US/Indiana-Starke

SystemV/CST6CDT

America/Merida

Canada/Saskatchewan

America/North_Dakota/New_Salem

America/Winnipeg

America/Panama

America/Indiana/Petersburg

America/Eirunepe

America/Grand_Turk

Cuba

Etc/GMT+5

Pacific/Easter

America/Fort_Wayne

America/Havana

America/Porto_Acre

US/Michigan

America/Louisville

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Guayaquil

America/Indiana/Vevay

America/Indiana/Vincennes

America/Indianapolis

America/Iqaluit

America/Kentucky/Louisville

EST5EDT

America/Nassau

America/Jamaica

America/Atikokan

America/Kentucky/Monticello

America/Coral_Harbour

America/Cayman

Chile/EasterIsland

America/Indiana/Indianapolis

America/Thunder_Bay

America/Indiana/Marengo

America/Bogota

SystemV/EST5

US/Eastern

Canada/Eastern

America/Port-au-Prince

America/Nipigon

Brazil/Acre

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

US/East-Indiana

America/Cancun

America/Lima

America/Rio_Branco

America/Detroit

Jamaica

America/Pangnirtung

America/Montreal

America/Indiana/Winamac

America/New_York

America/Toronto

SystemV/EST5EDT

America/Cuiaba

America/Marigot

Canada/Atlantic

Etc/GMT+4

America/Manaus

America/St_Thomas

America/Anguilla

America/Barbados

America/Curacao

America/Guyana

America/Martinique

America/Puerto_Rico

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Port_of_Spain

SystemV/AST4

America/Kralendijk

America/Antigua

America/Moncton

America/St_Vincent

America/Dominica

Atlantic/Bermuda

Brazil/West

America/Aruba

America/Halifax

America/La_Paz

America/Blanc-Sablon

America/Santo_Domingo

America/Glace_Bay

America/St_Barthelemy

America/St_Lucia

America/Montserrat

America/Lower_Princes

America/Thule

America/Tortola

America/Porto_Velho

America/Campo_Grande

America/Goose_Bay

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Virgin

America/Boa_Vista

America/Grenada

America/St_Kitts

America/Caracas

America/Guadeloupe

SystemV/AST4ADT

America/St_Johns

Canada/Newfoundland

Chile/Continental

America/Miquelon

America/Argentina/Catamarca

America/Argentina/Cordoba

America/Araguaina

America/Argentina/Salta

Etc/GMT+3

America/Montevideo

Brazil/East

America/Argentina/Mendoza

America/Argentina/Rio_Gallegos

America/Catamarca

America/Cordoba

America/Sao_Paulo

America/Argentina/Jujuy

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Cayenne

America/Recife

America/Buenos_Aires

America/Paramaribo

America/Mendoza

America/Santarem

America/Asuncion

America/Maceio

Atlantic/Stanley

Antarctica/Rothera

America/Argentina/San_Luis

America/Santiago

America/Argentina/Ushuaia

Antarctica/Palmer

America/Punta_Arenas

America/Fortaleza

America/Argentina/La_Rioja

America/Belem

America/Jujuy

America/Bahia

America/Argentina/San_Juan

America/Argentina/ComodRivadavia

America/Argentina/Tucuman

America/Rosario

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

America/Argentina/Buenos_Aires

Etc/GMT+2

America/Godthab

America/Noronha

Brazil/DeNoronha

Atlantic/South_Georgia

America/Scoresbysund

America/Nuuk

Etc/GMT+1

Atlantic/Cape_Verde

Atlantic/Azores

Pacific/Kiritimati

Etc/GMT-14

NZ-CHAT

Pacific/Chatham

Pacific/Fakaofo

Antarctica/McMurdo

Pacific/Enderbury

NZ

Pacific/Apia

Antarctica/South_Pole

Pacific/Kanton

Pacific/Auckland

Pacific/Tongatapu

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Etc/GMT-13

Pacific/Kwajalein

Pacific/Wallis

Pacific/Fiji

Pacific/Funafuti

Pacific/Nauru

Kwajalein

Pacific/Wake

Pacific/Norfolk

Pacific/Tarawa

Asia/Kamchatka

Etc/GMT-12

Asia/Anadyr

Pacific/Majuro

Australia/Hobart

Australia/Tasmania

Australia/ACT

Pacific/Ponape

Pacific/Bougainville

Australia/Victoria

Antarctica/Macquarie

Australia/Canberra

Australia/Currie

Australia/Lord_Howe

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/NSW

Pacific/Pohnpei

Pacific/Efate

Asia/Magadan

Pacific/Kosrae

Australia/Sydney

Australia/LHI

Asia/Sakhalin

Pacific/Noumea

Etc/GMT-11

Asia/Srednekolymsk

Australia/Melbourne

Pacific/Guadalcanal

Australia/Yancowinna

Australia/Adelaide

Australia/Broken_Hill

Australia/South

Pacific/Yap

Pacific/Port_Moresby

Pacific/Chuuk

Australia/Queensland

Pacific/Guam

Pacific/Truk

Asia/Vladivostok

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pacific/Saipan

Antarctica/DumontDUrville

Australia/Brisbane

Etc/GMT-10

Asia/Ust-Nera

Australia/Lindeman

Australia/North

Australia/Darwin

Etc/GMT-9

Pacific/Palau

Asia/Chita

Asia/Dili

Asia/Jayapura

Asia/Yakutsk

Asia/Pyongyang

ROK

Asia/Seoul

Asia/Khandyga

Japan

Asia/Tokyo

Australia/Eucla

Asia/Kuching

Asia/Chungking

Etc/GMT-8

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Australia/Perth

Asia/Macao

Asia/Macau

Asia/Choibalsan

Asia/Shanghai

Antarctica/Casey

Asia/Ulan_Bator

Asia/Chongqing

Asia/Ulaanbaatar

Asia/Taipei

Asia/Manila

PRC

Asia/Ujung_Pandang

Asia/Harbin

Singapore

Asia/Brunei

Australia/West

Asia/Hong_Kong

Asia/Makassar

Hongkong

Asia/Kuala_Lumpur

Asia/Irkutsk

Asia/Singapore

Asia/Pontianak

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Etc/GMT-7

Asia/Phnom_Penh

Asia/Novosibirsk

Antarctica/Davis

Asia/Tomsk

Asia/Jakarta

Asia/Barnaul

Indian/Christmas

Asia/Ho_Chi_Minh

Asia/Hovd

Asia/Bangkok

Asia/Vientiane

Asia/Novokuznetsk

Asia/Krasnoyarsk

Asia/Saigon

Asia/Yangon

Asia/Rangoon

Indian/Cocos

Asia/Kashgar

Etc/GMT-6

Asia/Dacca

Asia/Omsk

Asia/Dhaka

Indian/Chagos

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Asia/Bishkek

Asia/Urumqi

Asia/Thimbu

Asia/Thimphu

Asia/Kathmandu

Asia/Katmandu

Asia/Kolkata

Asia/Colombo

Asia/Calcutta

Asia/Aqtau

Etc/GMT-5

Asia/Samarkand

Asia/Almaty

Asia/Karachi

Asia/Yekaterinburg

Asia/Dushanbe

Indian/Maldives

Asia/Oral

Asia/Tashkent

Asia/Qostanay

Antarctica/Mawson

Asia/Qyzylorda

Asia/Aqtobe

Asia/Ashkhabad

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Antarctica/Vostok

Asia/Ashgabat

Asia/Atyrau

Indian/Kerguelen

Asia/Kabul

Asia/Yerevan

Etc/GMT-4

Asia/Dubai

Indian/Reunion

Indian/Mauritius

Europe/Saratov

Europe/Samara

Indian/Mahe

Asia/Baku

Asia/Muscat

Europe/Astrakhan

Asia/Tbilisi

Europe/Ulyanovsk

Iran

Asia/Tehran

Asia/Aden

Africa/Nairobi

Europe/Istanbul

Etc/GMT-3

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Indian/Comoro

Antarctica/Syowa

Africa/Mogadishu

Africa/Asmera

Asia/Istanbul

Europe/Moscow

Africa/Djibouti

Europe/Simferopol

Africa/Asmara

Asia/Baghdad

Asia/Damascus

Africa/Dar_es_Salaam

Africa/Addis_Ababa

Asia/Riyadh

Asia/Kuwait

Europe/Kirov

Africa/Kampala

Europe/Minsk

Asia/Qatar

Asia/Bahrain

Indian/Antananarivo

Indian/Mayotte

Europe/Volgograd

Turkey

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

W-SU

Asia/Amman

Africa/Cairo

Africa/Mbabane

Etc/GMT-2

Europe/Zaporozhye

Libya

Africa/Kigali

Africa/Tripoli

Israel

Europe/Kaliningrad

Africa/Windhoek

Europe/Bucharest

Europe/Mariehamn

Africa/Lubumbashi

Europe/Tiraspol

Europe/Chisinau

Europe/Helsinki

Asia/Beirut

Asia/Tel_Aviv

Europe/Sofia

Africa/Gaborone

Asia/Gaza

Europe/Riga

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Africa/Maputo

Europe/Uzhgorod

Asia/Jerusalem

Africa/Bujumbura

Europe/Kiev

Europe/Vilnius

Africa/Maseru

Africa/Blantyre

Africa/Lusaka

Africa/Harare

Europe/Tallinn

Africa/Khartoum

Africa/Johannesburg

Africa/Juba

Europe/Kyiv

Asia/Nicosia

Asia/Famagusta

EET

Asia/Hebron

Egypt

Europe/Nicosia

Europe/Athens

Europe/Brussels

Europe/Warsaw

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CET

Etc/GMT-1

Europe/Luxembourg

Africa/Tunis

Europe/Malta

Europe/Busingen

Africa/Malabo

Europe/Skopje

Europe/Sarajevo

Africa/Lagos

Europe/Rome

Africa/Algiers

Europe/Zurich

Europe/Gibraltar

Europe/Vaduz

Europe/Ljubljana

Europe/Berlin

Europe/Stockholm

Europe/Budapest

Europe/Zagreb

Europe/Paris

Africa/Ndjamena

Africa/Ceuta

Europe/Prague

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Europe/Copenhagen

Europe/Vienna

Europe/Tirane

MET

Europe/Amsterdam

Africa/Libreville

Africa/El_Aaiun

Europe/San_Marino

Africa/Douala

Africa/Brazzaville

Africa/Porto-Novo

Poland

Europe/Andorra

Europe/Oslo

Europe/Podgorica

Africa/Casablanca

Africa/Luanda

Atlantic/Jan_Mayen

Africa/Kinshasa

Europe/Madrid

Africa/Bangui

Europe/Belgrade

Africa/Niamey

Europe/Bratislava

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Arctic/Longyearbyen

Europe/Vatican

Europe/Monaco

Europe/London

GMT

Etc/GMT-0

Europe/Jersey

Atlantic/St_Helena

Europe/Guernsey

Europe/Isle_of_Man

Etc/GMT+0

Africa/Banjul

Etc/GMT

Africa/Freetown

GB-Eire

Africa/Bamako

GB

Africa/Conakry

Portugal

Universal

Africa/Sao_Tome

Africa/Nouakchott

Antarctica/Troll

UTC

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Etc/Universal

Atlantic/Faeroe

Africa/Abidjan

Eire

Africa/Accra

Atlantic/Faroe

Etc/UCT

GMT0

Europe/Dublin

Zulu

Africa/Ouagadougou

Atlantic/Reykjavik

Atlantic/Madeira

Etc/Zulu

Iceland

Europe/Lisbon

Atlantic/Canary

Africa/Lome

Greenwich

Europe/Belfast

Etc/GMT0

America/Danmarkshavn

Africa/Dakar

Africa/Bissau

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

WET

Etc/Greenwich

Africa/Timbuktu

UCT

Africa/Monrovia

Etc/UTC

Network Discovery Configuration

This API is used to list a specific network discovery configuration.

Understanding the Sample URL

- **IP/HostName/TenantName:** Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
- **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication.

  The IP address will be included in the endpoint URL for an on-prem deployment.
- **HostName**: A human-readable label assigned to a device (host) on a network.

  The hostname will be included in the endpoint URL for an on-prem deployment.
- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify.

  The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT:** AppViewX gateway port.

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: 31443.
  - **avxapi**:Path parameter value (static) that is part of the endpoint's URL
  - **Endpoint**:Endpoint of the API, for example: execute-hook
  - **gwsource**:Source or origin of a gateway, for example: external.
- Create a Network
- Get a Network

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• List a Network
• Update a Network
• Delete a Network

Create a Network

The API creates a network entry in discovery configuration based on the payload.

.

Before you Begin

• The user should have permission to create/modify network entries.

Request Structure

Endpoint:	/certificate/discovery/networks
Type:	POST
Action:	network-create
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
username *Header*	(Mandatory) Username for logging in to AppViewX. **Type**: String
password *Header*	(Mandatory) Password for logging in to AppViewX. **Type**: String
Content-Type	(Mandatory) Payload content-type with application/json value. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) Source from which the request is triggered. (For example. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
name	(Mandatory) name of the network entry. **Type**: String **Constraint**: • Name must be at least 3 characters • Name cannot exceed 255 characters • Name cannot start with special characters or numbers • Name must not have the special characters (<, >, &, %, ', "). **Recommanded**: It is recommended to not use the following special characters: (<, >, (,), $, &, |, /, `, [,], {, }, ?, ;, ~ , !, %, ', ", \).
description	(Optional) description for the network entry. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraints: • Description cannot exceed 500 characters. • Description must not have '<' character.
settings	(Mandatory) network setting that needs to be associated with the network entry. **Note:** The provided network settings must be available. **Type**: String
networks	(Mandatory) The list of network endpoints that are included in the network entry. **Type**: networks
network	(Mandatory) network to be added in the network entry. **Note:** Can have IP range, subnet, individual IP. **Type**: String
dataCenter	(Mandatory) dataCenter for the network. **Note:** The provided data center must be available. **Type**: String
sniHostname	(Optional) comma separated SNI Hostnames for the network. **Type**: String **Constraint**: sniHostname must not have '<' character

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response for the group creation operation **Type**: Boolean
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
400 Bad Request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request


```
{
  "name": "BLR_network",
  "description": "network to be added",
  "settings": "Default",
  "networks": [
    {
      "network": "192.168.220.120",
      "dataCenter": "absecon",
      "sniHostname": "appviewx.com"
    }
  ]
}
```


Sample Response


```
{
  "response": "Success",
  "message": "Successfully created the network",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Get a Network

The API gets the network entry in discovery configuration from the id or name.

.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you Begin

• The user should have permission to view network entries.

Request Structure

Endpoint:	/certificate/discovery/networks
Type:	GET
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/networks?id=<id>&gwsource=external https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/networks?name=<name>&gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
username *Header*	(Mandatory) Username for logging in to AppViewX. **Type**: String
password *Header*	(Mandatory) Password for logging in to AppViewX. **Type**: String
Content-Type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) Source from which the request is triggered. (For example. external) **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains the response for the group creation operation **Type**: Boolean
id	Unique identifier for the network entry. **Type**: String
name	Name of the network entry. **Type**: String
description	Description of the network entry. **Type**: String
status	Status of the network entry. **Type**: Boolean
readOnly	Read only access for the network entry. **Type**: Boolean
createdDate	Creation date of the network entry. **Type**: Long
updatedDate	Updation date of the network entry. **Type**: Long
createdBy	User who created the network entry. **Type**: String
updatedBy	User who updated the network entry. **Type**: String
settings	Network setting associated with the network entry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
networks	List of network endpoints. **Type**: networks
network	Network endpoint (IP, Subnet, and IP range). **Type**: String
status	Status of the network endpoint. **Type**: String
dataCenter	Datacenter for the the network endpoint. **Type**: String
sniHostname	SNI hostname for the network endpoint. **Type**: String
uniqueId	Unique id for the network endpoint. **Type**: Long
scheduledDiscovery	List of scheduled discovery names done with the network entry. **Type**: List
onDemandDiscovery	List of ondemand discovery names done with the network entry. **Type**: List
dataCenter	List of datacenter for the network entry. **Type**: List
message	Success message or failure description in case of error. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
400 Bad Request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request

No payload for GET request.

Sample Response


```
{
  "response": {
    "id": "6839962c0e2cab59aa01c5fb",
    "name": "test-network",
    "description": "network to be added",
    "status": true,
    "readOnly": false,
    "createdDate": 1748604460852,
    "updatedDate": 1748604460852,
    "createdBy": "admin",
    "updatedBy": "admin",
    "settings": "Default",
    "networks": [
      {
        "network": "1.1.1.1",
        "endpoints": null,
        "ports": null,
        "status": "Valid",
        "reason": null,
        "dataCenter": "absecon",
        "sniHostname": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "settings": null,
            "uniqueId": 1748604460849
        }
    ],
    "scheduledDiscovery": [],
    "onDemandDiscovery": [
        "discovery-test"
    ],
    "dataCenter": [
        "absecon"
    ],
    "ids": null
  },
  "message": "Network fetched successfully with network name.",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

List a Network

The API lists the network entries in discovery configuration based on the payload.

.

Before you Begin

- The user should have permission to view network entries.

Request Structure

Endpoint:	/certificate/discovery/networks
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
username *Header*	(Mandatory) Username for logging in to AppViewX. **Type**: String
password	(Mandatory) Password for logging in to AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String
Content-Type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) Source from which the request is triggered. (For example. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
start	(Optional) Specifies the zero-based index of the first item to return. **Type**: Integer **Constraint**: start must not be negative **Default**: Zero (0).
max	(Optional) Specifies the maximum number of items to return. **Type**: Integer **Constraints**: max must not be negative **Default**: 100 (if the provided value exceeds 100).
filter	(Optional) Free text search to filter the list of networks. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
sortColumn	(Optional) Specifies the field by which to sort the results. **Type**: String **Possible Value(s)**: "name", "description", "scheduledDiscovery", "onDemandDiscovery", "dataCenter", "settings" **Default**: name
sortOrder	(Optional) Defines the sort direction. **Type**: String **Possible Value(s)**: Must be one of “asc” or “desc”.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response for the group creation operation **Type**: Boolean
search	The search string entered in the “filter” field of payload. **Type**: String
totalRecords	The total network entries present in the database for the free text search filter. **Type**: long
data	Contains the list of network entries. **Type**: List
id	Unique identifier for the network entry. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
name	Name of the network entry. **Type**: String
description	Description of the network entry. **Type**: String
status	Status of the network entry. **Type**: Boolean
readOnly	Read only access for the network entry. **Type**: Boolean
createdDate	Creation date of the network entry. **Type**: Long
updatedDate	Updation date of the network entry. **Type**: Long
createdBy	User who created the network entry. **Type**: String
updatedBy	User who updated the network entry. **Type**: String
settings	Network setting associated with the network entry. **Type**: String
scheduledDiscovery	List of scheduled discovery names done with the network entry. **Type**: List
onDemandDiscovery	List of ondemand discovery names done with the network entry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: List
dataCenter	List of datacenter for the network entry. **Type**: List
executionTime	Indicates the time at which the execution was triggered. **Type**: Long
iTotalDisplayRecords	The total network entries present in the database for the free text search filter. **Type**: Long
message	Success message or failure description in case of error. **Failure:** Returns the Failure message **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
400 Bad Request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request

```
{
  "start" : 0,
  "max" : 10,
  "filter" : "",
  "sortColumn":"name",
  "sortOrder":"desc"
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Response


```
{
  "response": {
    "search": "",
    "totalRecords": 2,
    "data": [
      {
        "id": "683c38170b80a91c95bea252",
        "name": "test-networks12",
        "description": "network to be added",
        "status": true,
        "readOnly": false,
        "createdDate": 1748776983876,
        "updatedDate": 1748776983876,
        "createdBy": "admin",
        "updatedBy": "admin",
        "settings": "Default",
        "scheduledDiscovery": [],
        "onDemandDiscovery": [],
        "dataCenter": [
          "absecon"
        ],
        "ids": null
      }
    ],
    "autoSuggest": null,
    "executionTime": 1748779898,
    "iTotalDisplayRecords": 2
  },
  "message": "Networks are listed",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Update a Network

The API updates a network entry in discovery configuration based on the payload.

.

Before you Begin

- The user should have permission to view network entries.

Request Structure

Endpoint:	/certificate/discovery/networks
Type:	PUT
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?gwsource=external

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To understand the elements of the sample URL, click here.
Headers
Content-Type: application/json

Input Parameters

Name	Description
username *Header*	(Mandatory) Username for logging in to AppViewX. **Type**: String
password *Header*	(Mandatory) Password for logging in to AppViewX. **Type**: String
Content-Type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) Source from which the request is triggered. (For example. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
id	(Mandatory) ID of the network entry to be updated. **Type**: String
description	Description of the network entry. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraints: • description cannot exceed 500 characters. • description must not have '<' character.
settings	(Optional) network setting that needs to be associated with the network entry. **Note:** The provided network settings must be available. **Type**: String
status	Status of the network entry. **Type**: Boolean
networks	(Optional) The list of network endpoints that needs to be updated in the network entry. **Type**: networks
network	(Mandatory) network to be added in the network entry. **Note:** Can have ip range, subnet, individual IP. **Type**: String
dataCenter	(Mandatory) dataCenter for the network. **Note:** The provided data center must be available. **Type**: String
sniHostname	(Optional) comma separated SNI Hostnames for the network. **Type**: String **Constraints:** sniHostname must not have '<' character.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload-Networks

Payload

Name	Description
network	(Mandatory) network to be added in the network entry. **Note:** Can have ip range, subnet, individual IP. **Type**: String
dataCenter	(Mandatory) dataCenter for the network. **Note:** The provided data center must be available. **Type**: String
sniHostname	(Optional) comma separated SNI Hostnames for the network. **Type**: String **Constraints:** sniHostname must not have '<' character.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response for the group creation operation **Type**: Boolean
message	Success message or failure description in case of error. **Failure:** Returns the Failure message **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
400 Bad Request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request


```
{
  "id": "683c3b3c0b80a91c95bea325",
  "description": "",
  "settings": "Default",
  "status": true,
  "networks": [
    {
      "network": "192.168.220.120",
      "dataCenter": "absecon",
      "sniHostname": "appviewx.com"
    }
  ]
}
```


Sample Response


```
{
  "response": "Success",
  "message": "Successfully updated the network",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Delete a Network

The API deletes the network entries in discovery configuration based on the list of ids.

.

Before you Begin

- The user should have permission to view network entries.

Request Structure

Endpoint:	/certificate/discovery/networks

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
username *Header*	(Mandatory) Username for logging in to AppViewX. **Type**: String
password *Header*	(Mandatory) Password for logging in to AppViewX. **Type**: String
Content-Type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) Source from which the request is triggered. (For example. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
ids	(Mandatory) list of network ids, that needs to be deleted

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: list

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Returns “Success” on successful updation of network. **Type**: Boolean
message	Returns “Network(s) deleted successfully”. **Failure:** Returns the Failure message **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
400 Bad Request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request

```
{
  "ids": [
    "683c3b3c0b80a91c95bea325"
  ]
}
```

Sample Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
  "response": "Success",
  "message": "Network(s) deleted successfully",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Fetch Single Certificate Discovery

This API is used to list a specific discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

• The user should have the ACF permission to view the certificate discovery.

Request Structure

Endpoint:	/certificate/discovery/instance?discoveryName=<name>
Type:	GET
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?discoveryName=<name>&gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.
id response	Unique identifier for the discovery object. **Type:** String
name response	Name of the discovery instance. **Type:** String
type response	Type of discovery such as e.g.: On-demand, Scheduled, Managed. **Type:** String
source response	Source of the discovery eg: IP range, Upload, etc. **Type:** String
syncStatus response	Status indicating whether the certificate is managed or monitored. **Type:** String
groupName response	Group name of the discovery instance under which it is categorized. **Type:** String
dicoverCount response	Count of discovered certificates. **Type:** Integer
passwordCertCountresponse	Count of certificates that are protected by a password. **Type:** Integer
encryptedPrivateKeyCount response	Count of certificates with encrypted private keys. **Type:** Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
mergedCount response	Total number of merged certificates during the discovery process. **Type:** Integer
status response	Overall status of the discovery instance. Eg: success, failure or in-progress **Type:** String
statusMessage response	Message providing additional information about the status of the discovery process. **Type:** String
passiveMode response	X **Type:** Boolean (true/false)
startTime response	Time when the discovery instance was initiated (DD/MM/YY HH:MM). **Type:** Date/time
endTime response	Time when the discovery completed (DD/MM/YY HH:MM). **Type:** Date/time
associatedRule response	Discovery rule associated with the discovery instance. **Type:** String
discoverAllCerts response	Determines if all certificates were discovered. **Type:** Boolean (true/false)
customDirectoryNames response	Custom directory names specified for the discovery instance. **Type:** String
totalCertCount	Total number of certificates discovered in the instance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type:** Integer
filters response	Specifies the criteria for simplifying the discovery process. **Type:** Object
startDate response.filters	Start date for filtering the discovery instance. **Type:** Date/time
endDate response.filters	End date for filtering the discovery instance. **Type:** Date/time
discoverBy response.filters	Method or criteria used to discover the certificates. **Type:** String
caNames response.filters	List of Certificate Authority names from which certificates are discovered (If **discoverBy** field value is **CA**). **Type:** List of String
regions response.filters	Regions considered during the discovery process. **Type:** List of String
vendorSpecificConditions response.filters	Conditions specific to the vendor for the discovery process. **Type:** Object
certStatus response.filters.vendorSpecificConditions	List of certificate statuses to filter by. **Type:** List of String
certTypes response.filters.vendorSpecificConditions	List of certificate types to filter by. **Type:** List of String
message	Displays the number of records found if success or a failure message.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type:** String
tags	Additional information in case of failure response.
headers	HTTP headers associated with the response. **Type:** String

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Accepted.
400 Bad Request	ERR_DISC_DISCOVERY_HISTORY_RETRIVAL	Error while retrieving discovery history. **Remediation**: Discovery name passed in the request should be present in the database.
400 Bad Request	NO_RECORDS_FOUND	No matching records found. **Remediation**: Discovery name passed in the request should be present in the system.
417 Expectation failed	MANDATORY_QUERY_PARAM_MISSING	Mandatory query param is missing or invalid. **Remediation**: The parameter <discoveryName> must be present in the URL request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	CERT-FV-001	Invalid query param found for discoveryName. **Remediation**: The discoveryName value should be a minimum of 2 characters.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload

No payload for GET request.

Response


```
{
   "response": {
      "id": "666156a4afa237151d466af7",
      "name": "googleCAScan",
      "type": "ONDEMAND",
      "source": "Certificate Authorities",
      "syncStatus": "Managed",
      "groupName": "Default",
      "discoverCount": 0,
      "passwordCertCount": 0,
      "encryptedPrivateKeyCount": 0,
      "mergedCount": 9661,
      "status": "Success",
      "statusMessage": "Discovery Completed Successfully",
      "passiveMode": false,
      "startTime": "06/06/24 06:26:44",
      "endTime": "06/06/24 06:39:37",
      "associatedRule": "",
      "discoverAllCerts": true,
      "customDirectoryNames": null,
      "totalCertCount": 9661,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "filters": {
        "startDate": 0,
        "endDate": 0,
        "discoverBy": "CA",
        "caNames": [
          "us-east1:Google-External-CA",
          "us-east1:SplunkLab"
        ],
        "regions": null,
        "vendorSpecificConditions": {
          "certStatus": [],
          "certTypes": []
        }
      }
    },
    "message": "Summary view fetched successfully with discovery name.",
    "appStatusCode": null,
    "tags": {},
    "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Fetch Certificate Discovery Results **by Discovery Name**

The API enables users to fetch the discovered certificates from a particular discovery instance using the discovery name.

Before you begin

- The user should have the ACF permission to view the certificate discovery.

Request Structure

Endpoint:	/certificate/discovery/instance?discoveryName=<name>
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?discoveryName=<name>&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session ID received after login.
Header	**Type**: String **Constraints**: Required if **username** and **password** are not provided.
userName	(Mandatory) Username that is configured in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String
password	(Mandatory) Password of that user.
Header	**Type**: String
content-type	(Mandatory) Payload content-type with application/json value.
Header	**Type**: String **Constraint**: The value must be **application/json**.
gwsource	(Mandatory) The source from which the request is triggered, e.g., external.
Query	**Type**: String
Payload*Body*	Contains all the parameters to be sent in the request body for the post request.
	Type: Payload

Payload

Payload

Name	Description
name	(Mandatory) Name of the discovery instance to be created. **Type**: String
searchTextValue	(Optional) Query the fetched results based on the provided search value.
startIndex	(Optional) specify the start index from where the certificate data has to be fetched.
sortColumn	(Optional) specifies the column on which the sort has to be applied.
sortOrder	(Optional) specifies the sort order to be applied. **Constraint:** Possible values : 1, -1, asc, desc
maxSize	(Optional) specifies the maximum number of results that can be retrieved.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint : Possible values in the range 1 to 1000.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes. **Type:** A JSON object
search	null
totalRecords	Total number of records in the specified discoveryInstance.
data	Certificate metadata. **Type**: Array of Certificate json String
autoSuggest	null
executionTime	Execution time of the request.
iTotalDisplayRecords	Total number of records in the specified discoveryInstance.
message	If matching records are found for the search query - null. If no records are available for the search query - No matching records found. **Type:** String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type:** String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Accepted.
400 Bad Request	ERR_DISC_DISCOVERY_HISTORY_RETRIVAL	Error while retrieving discovery history. **Remediation**: Discovery name passed in the request should be present in the database.
400 Bad Request	NO_RECORDS_FOUND	No matching records found. **Remediation**: Discovery name passed in the request should be present in the system.
417 Expectation failed	MANDATORY_QUERY_PARAM_MISSING	Mandatory query param is missing or invalid. **Remediation**: The parameter <discoveryName> must be present in the URL request.
417 Expectation failed	CERT-FV-001	Invalid query param found for discoveryName. **Remediation**: The discoveryName value should be a minimum of 2 characters.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload

```
{
  "searchTextValue": "",
  "startIndex": 0,
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "sortColumn": "none",
  "sortOrder": "desc",
  "name": "test #1",
  "maxSize": 5
}
```


Response


```
{
  "response": {
    "search": null,
    "totalRecords": 6,
    "data": [
      {
        "commonName": "pe-cert-swat-n12.lab.appviewx.net-ca@1749432603",
        "serialNumber": "61:14:84:02:1B:C9:73:8F",
        "serialNumberHex": "611484021bc9738f",
        "issuerCommonName": "pe-cert-swat-n12.lab.appviewx.net-ca@1749432603",
        "status": null,
        "avxStatus": "Discovered",
        "associatedObjects": [],
        "discoverySources": [
          "pe-cert-swat-120.lab.appviewx.net:10250"
        ],
        "subjectOrganization": "",
        "subjectOrganizationUnit": "",
        "subjectLocality": "",
        "subjectState": "",
        "subjectCountry": "",
        "issuerOrganization": "",
        "issuerOrganizationUnit": "",
        "issuerLocality": "",
        "issuerState": "",
        "issuerCountry": "",
        "version": "3",
        "validFrom": 1749429003000,
        "validTo": 1780965003000,
        "firstDiscoveryDate": 1749446451605,
        "lastBeforeDiscoveryDate": 1749446451605,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"lastDiscoveryDate": 1749446451605,
"firstDiscoveryDateStr": null,
"lastBeforeDiscoveryDateStr": null,
"validFor": "364 day(s) 18 hr(s) 52 min(s)",
"keyAlgorithmAndSize": "RSA 2048",
"signatureAlgorithm": "SHA256withRSA",
"signatureHashAlgorithm": null,
"keyUsage": "DigitalSignature, KeyEncipherment, keyCertSign",
"extendedKeyUsage": "",
"basicConstraints": "Subject Type=CA, Path Length=none",
"group": null,
"subjectAlternativeNames": [],
"complianceStatus": "",
"applications": [
    "192.168.220.120:10250"
],
"policyIdentifiers": [],
"expiryStatus": "Valid",
"permission": null,
"category": "Root CA",
"uuid": "35357988706e58f8ce0da089df6b8e21dc0ca26b",
"id": null,
"certificateAuthority": "OTHERS",
"authorityKeyIdentifier": "",
"subjectKeyIdentifier": "BF:DD:9E:7F:86:30:9F:9C:8D:05:5C:CB:33:4B:9B:65:14:71:23:A6",
"issuerSerialNumber": null,
"authorityInfoAccess": [],
"certificatePolicies": [],
"crlDistributionPoints": [],
"thumbprintAlgorithm": null,
"thumbPrint": "50:7C:CD:47:DB:65:32:92:B8:C7:0B:BC:87:05:5F:7F:9D:D2:5F:96",
"type": "Self Signed",
"genericFields": null,
"certAttributes": null,
"customAttributes": null,
"validFromDate": null,
"validToDate": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "discoveredFileNames": [],
            "issuingTemplate": null,
            "csrGenerationSource": null,
            "certificateHSMDetails": null,
            "deviceDetails": null,
            "newConnectors": [
                "192.168.220.120:10250:absecon"
            ],
            "csrAvailable": false,
            "enhancedSANTypes": null,
            "autoRenewDate": null,
            "autoRegenDate": null,
            "missingParamsForAutoRenew": null,
            "base64ImageContent": null,
            "caConnectorName": null,
            "caSettingName": null,
            "suspendedCertificate": false,
            "comments": null,
            "mailAddress": "",
            "streetAddress": null,
            "postalCode": null,
            "publicKeyModulus": null,
            "requestIds": null,
            "orderId": null,
            "publicKey":
 "30:82:01:0A:02:82:01:01:00:F5:B0:8E:D0:15:51:02:5B:06:64:06:1C:14:50:41:1A:C1:FE:6F:D5:0A:2E:49:FE:49:3B:9D:6A:3A:92:07:6D:15:50:06:AB:B3:18:D4:D
4:7F:E3:88:DD:EA:19:70:7B:56:90:0D:02:0D:25:1D:95:20:61:9A:4A:CD:4A:DE:C6:C1:C1:E3:94:EA:5D:BB:28:FA:89:25:82:2C:55:97:5A:48:5C:F8:B2:6C:DF:5A:0
1:C0:C0:C9:DF:33:B2:50:F3:35:A8:46:5A:44:66:7B:36:E8:62:7F:C3:6B:94:A5:60:D6:F2:CD:FD:55:29:1F:5A:6B:F4:86:4F:3B:19:EC:26:90:FB:AC:39:90:94:DD:A7
:D3:75:E1:A5:C3:13:42:64:66:1C:ED:35:87:91:B0:E5:E1:A5:4E:54:EA:47:C8:51:53:B6:BA:F4:FA:67:EB:39:82:CF:F5:7B:B5:B4:E5:00:8B:31:74:3C:BA:17:93:02:
D0:E0:1D:92:F6:DC:A4:B6:1A:30:D4:DB:23:1A:B4:91:5E:ED:D7:79:A8:65:4A:3C:24:55:12:88:BF:56:B1:50:CC:2B:52:0E:62:09:D2:93:4B:4F:22:0F:D2:5B:28:64:9
5:89:15:5C:12:33:0F:AC:A9:A1:EC:56:E2:58:29:AD:AF:64:81:F0:94:BF:B0:D3:02:03:01:00:01",
            "ellipticCurve": null,
            "issuedByRootCertificate": false,
            "cumulativeSanCount": 0,
            "chainPriority": 0,
            "caCertificateType": null,
            "templateProfile": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "certificateTags": null,
    "resourceTags": null,
    "ocspStatus": null,
    "enrollmentMethod": null,
    "kubeService": null,
    "subject": "CN=pe-cert-swat-n12.lab.appviewx.net-ca@1749432603",
    "discoveryTypes": null,
    "certLifeCycleAction": null,
    "certLifeCycleActionTimestamp": 0,
    "isSsoActive": null,
    "customExtensions": null,
    "privatekeyAvaliable": false,
    "cvss": null
},
{
    "commonName": "kube-apiserver",
    "serialNumber": "4D:81:8A:DF:5A:7C:C2:1E",
    "serialNumberHex": "4d818adf5a7cc21e",
    "issuerCommonName": "kubernetes",
    "status": null,
    "avxStatus": "Discovered",
    "associatedObjects": [],
    "discoverySources": [
        "pe-cert-swat-120.lab.appviewx.net:6443"
    ],
    "subjectOrganization": "",
    "subjectOrganizationUnit": "",
    "subjectLocality": "",
    "subjectState": "",
    "subjectCountry": "",
    "issuerOrganization": "",
    "issuerOrganizationUnit": "",
    "issuerLocality": "",
    "issuerState": "",
    "issuerCountry": "",
    "version": "3",
    "validFrom": 1749432296000,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"validTo": 1780968596000,
"firstDiscoveryDate": 1749446451563,
"lastBeforeDiscoveryDate": 1749446451563,
"lastDiscoveryDate": 1749446451563,
"firstDiscoveryDateStr": null,
"lastBeforeDiscoveryDateStr": null,
"validFor": "364 day(s) 19 hr(s) 52 min(s)",
"keyAlgorithmAndSize": "RSA 2048",
"signatureAlgorithm": "SHA256withRSA",
"signatureHashAlgorithm": null,
"keyUsage": "DigitalSignature, KeyEncipherment",
"extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) ",
"basicConstraints": "Subject Type=End entity, Path Length=none",
"group": null,
"subjectAlternativeNames": [
    "DNS : kubernetes, kubernetes.default, kubernetes.default.svc, kubernetes.default.svc.cluster.local, pe-cert-swat-n12.lab.appviewx.net",
    "IP Address : 10.96.0.1, 192.168.220.120"
],
"complianceStatus": "",
"applications": [
    "192.168.220.120:6443"
],
"policyIdentifiers": [],
"expiryStatus": "Valid",
"permission": null,
"category": "Server",
"uuid": "9a68c5f9c0302f0bae673baa4d2fe23f66f213ee",
"id": null,
"certificateAuthority": "OTHERS",
"authorityKeyIdentifier": "64:B5:37:9B:3B:ED:7E:74:9A:41:FA:8B:7F:E1:6B:49:A5:9A:93:0E",
"subjectKeyIdentifier": "",
"issuerSerialNumber": null,
"authorityInfoAccess": [],
"certificatePolicies": [],
"crlDistributionPoints": [],
"thumbprintAlgorithm": null,
"thumbPrint": "3E:4C:F9:1C:A0:24:CD:19:58:F1:81:D6:59:34:F5:25:AF:A5:A2:BA",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "type": "Others",
        "genericFields": null,
        "certAttributes": null,
        "customAttributes": null,
        "validFromDate": null,
        "validToDate": null,
        "discoveredFileNames": [],
        "issuingTemplate": null,
        "csrGenerationSource": null,
        "certificateHSMDetails": null,
        "deviceDetails": null,
        "newConnectors": [
            "192.168.220.120:6443:absecon"
        ],
        "csrAvailable": false,
        "enhancedSANTypes": null,
        "autoRenewDate": null,
        "autoRegenDate": null,
        "missingParamsForAutoRenew": null,
        "base64ImageContent": null,
        "caConnectorName": null,
        "caSettingName": null,
        "suspendedCertificate": false,
        "comments": null,
        "mailAddress": "",
        "streetAddress": null,
        "postalCode": null,
        "publicKeyModulus": null,
        "requestIds": null,
        "orderId": null,
        "publicKey":
 "30:82:01:0A:02:82:01:01:00:A6:46:A0:B7:26:5A:B6:E3:07:91:1B:C2:12:8B:C2:F3:ED:77:D0:38:67:88:55:F4:B1:17:12:4C:58:BA:1F:93:F4:C8:FC:72:7F:C6:95:84
:00:B7:7E:45:3B:21:A8:F3:0A:01:F7:CD:6E:EE:46:4D:9D:2C:D4:75:72:49:34:12:9C:9E:ED:BC:5E:20:24:DA:9E:A4:59:F9:47:3E:20:6F:6C:83:19:73:50:7E:F9:5D:
72:85:11:37:38:4C:8E:5D:34:76:9D:D4:EC:6E:B3:C0:B6:E5:54:FA:B8:BF:80:6B:E2:A6:CA:9A:6F:9D:7F:C6:AB:55:3C:54:02:6F:97:C1:26:5F:75:1C:B7:7F:6D:F3:
6D:E6:3A:33:4D:49:A0:15:E4:A7:52:DE:7A:B6:A8:C7:0E:C9:90:61:77:E9:94:AB:3E:58:CE:B1:12:8C:0A:3A:DE:92:2E:B3:03:AE:93:B7:38:3F:50:0F:46:16:E6:BE:
F2:08:91:0F:1F:97:86:23:A5:6F:08:32:A4:80:43:49:07:2F:EE:1D:B7:6F:B6:5A:9D:A8:3A:E8:00:2C:3C:47:32:66:AE:D5:F8:5A:F9:5C:53:5C:40:59:D3:F1:34:74:9E:
57:30:32:8B:87:FF:8C:18:B6:32:E1:DC:C5:21:01:BF:2D:B0:7F:60:A5:77:01:02:03:01:00:01",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "ellipticCurve": null,
        "issuedByRootCertificate": false,
        "cumulativeSanCount": 7,
        "chainPriority": 0,
        "caCertificateType": null,
        "templateProfile": null,
        "certificateTags": null,
        "resourceTags": null,
        "ocspStatus": null,
        "enrollmentMethod": null,
        "kubeService": null,
        "subject": "CN=kube-apiserver",
        "discoveryTypes": null,
        "certLifeCycleAction": null,
        "certLifeCycleActionTimestamp": 0,
        "isSsoActive": null,
        "customExtensions": null,
        "privatekeyAvaliable": false,
        "cvss": null
    },
    {
        "commonName": "pe-cert-swat-n12.lab.appviewx.net",
        "serialNumber": "30:46:50:C9:E5:D2:BC:F2",
        "serialNumberHex": "304650c9e5d2bcf2",
        "issuerCommonName": "etcd-ca",
        "status": null,
        "avxStatus": "Discovered",
        "associatedObjects": [],
        "discoverySources": [
            "pe-cert-swat-120.lab.appviewx.net:2379"
        ],
        "subjectOrganization": "",
        "subjectOrganizationUnit": "",
        "subjectLocality": "",
        "subjectState": "",
        "subjectCountry": "",
        "issuerOrganization": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"issuerOrganizationUnit": "",
"issuerLocality": "",
"issuerState": "",
"issuerCountry": "",
"version": "3",
"validFrom": 1749432296000,
"validTo": 1780968596000,
"firstDiscoveryDate": 1749446451563,
"lastBeforeDiscoveryDate": 1749446451563,
"lastDiscoveryDate": 1749446451563,
"firstDiscoveryDateStr": null,
"lastBeforeDiscoveryDateStr": null,
"validFor": "364 day(s) 19 hr(s) 52 min(s)",
"keyAlgorithmAndSize": "RSA 2048",
"signatureAlgorithm": "SHA256withRSA",
"signatureHashAlgorithm": null,
"keyUsage": "DigitalSignature, KeyEncipherment",
"extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2) ",
"basicConstraints": "Subject Type=End entity, Path Length=none",
"group": null,
"subjectAlternativeNames": [
    "DNS : localhost, pe-cert-swat-n12.lab.appviewx.net",
    "IP Address : 192.168.220.120, 127.0.0.1, 0:0:0:0:0:0:0:1"
],
"complianceStatus": "",
"applications": [
    "192.168.220.120:2379"
],
"policyIdentifiers": [],
"expiryStatus": "Valid",
"permission": null,
"category": "Server",
"uuid": "b00604248e42ca27619267cb4be53c423f352f79",
"id": null,
"certificateAuthority": "OTHERS",
"authorityKeyIdentifier": "EC:4C:44:44:4B:62:6D:08:DD:06:33:69:12:2B:9C:2E:06:89:61:C8",
"subjectKeyIdentifier": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "issuerSerialNumber": null,
    "authorityInfoAccess": [],
    "certificatePolicies": [],
    "crlDistributionPoints": [],
    "thumbprintAlgorithm": null,
    "thumbPrint": "3B:F3:5D:78:C4:F7:82:9D:46:33:BE:B4:14:56:C2:96:D3:92:62:DE",
    "type": "Others",
    "genericFields": null,
    "certAttributes": null,
    "customAttributes": null,
    "validFromDate": null,
    "validToDate": null,
    "discoveredFileNames": [],
    "issuingTemplate": null,
    "csrGenerationSource": null,
    "certificateHSMDetails": null,
    "deviceDetails": null,
    "newConnectors": [
        "192.168.220.120:2379:absecon"
    ],
    "csrAvailable": false,
    "enhancedSANTypes": null,
    "autoRenewDate": null,
    "autoRegenDate": null,
    "missingParamsForAutoRenew": null,
    "base64ImageContent": null,
    "caConnectorName": null,
    "caSettingName": null,
    "suspendedCertificate": false,
    "comments": null,
    "mailAddress": "",
    "streetAddress": null,
    "postalCode": null,
    "publicKeyModulus": null,
    "requestIds": null,
    "orderId": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "publicKey":
 "30:82:01:0A:02:82:01:01:00:B4:FF:0B:D2:38:0C:ED:F4:1A:52:46:FF:21:35:1F:1B:45:81:86:85:39:55:46:7C:E1:00:6B:A2:7C:33:79:21:57:6E:14:C0:3D:F2:AA:59
:9D:0B:F0:82:BF:01:4D:86:47:4A:5F:81:D9:45:73:CC:FE:6D:D0:39:F4:17:1D:5E:60:B4:FA:2F:C9:23:EE:2F:47:FA:29:62:E1:D6:66:F6:D3:A5:92:74:25:FE:A1:DC:
82:45:72:52:9E:C3:99:C5:BD:07:61:54:07:EC:93:BF:B0:5D:6F:F3:39:73:F5:B0:07:B4:CE:51:96:41:73:F3:AC:51:19:0A:1D:02:79:4A:41:82:7E:D6:3C:B2:B2:B4:53
:16:8F:C0:84:0B:D4:64:42:C6:22:83:51:94:B2:B2:88:36:8C:ED:D3:25:1F:EC:D4:5D:8F:2F:C1:99:87:EE:D2:60:4B:47:00:25:57:9C:BD:51:D2:CA:4B:B6:D3:04:51:
D1:E6:3B:1D:3F:3B:7E:5A:02:67:69:40:25:46:21:69:B4:BF:49:67:FD:1C:D7:39:21:03:14:AB:81:06:F2:83:85:F2:F1:B7:DC:85:2F:E9:8D:54:85:C0:F2:69:93:9C:41:
99:8E:FA:C1:74:E6:FE:26:88:0B:DD:DF:99:23:94:CF:96:03:D1:9E:B1:B3:02:03:01:00:01",
            "ellipticCurve": null,
            "issuedByRootCertificate": false,
            "cumulativeSanCount": 5,
            "chainPriority": 0,
            "caCertificateType": null,
            "templateProfile": null,
            "certificateTags": null,
            "resourceTags": null,
            "ocspStatus": null,
            "enrollmentMethod": null,
            "kubeService": null,
            "subject": "CN=pe-cert-swat-n12.lab.appviewx.net",
            "discoveryTypes": null,
            "certLifeCycleAction": null,
            "certLifeCycleActionTimestamp": 0,
            "isSsoActive": null,
            "customExtensions": null,
            "privatekeyAvaliable": false,
            "cvss": null
        },
        {
            "commonName": "pe-cert-swat-n12.lab.appviewx.net@1749432603",
            "serialNumber": "0E:ED:A6:17:67:F1:F1:B0",
            "serialNumberHex": "0eeda61767f1f1b0",
            "issuerCommonName": "pe-cert-swat-n12.lab.appviewx.net-ca@1749432603",
            "status": null,
            "avxStatus": "Discovered",
            "associatedObjects": [],
            "discoverySources": [
                "pe-cert-swat-120.lab.appviewx.net:10250"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
],
"subjectOrganization": "",
"subjectOrganizationUnit": "",
"subjectLocality": "",
"subjectState": "",
"subjectCountry": "",
"issuerOrganization": "",
"issuerOrganizationUnit": "",
"issuerLocality": "",
"issuerState": "",
"issuerCountry": "",
"version": "3",
"validFrom": 1749429003000,
"validTo": 1780965003000,
"firstDiscoveryDate": 1749446451563,
"lastBeforeDiscoveryDate": 1749446451563,
"lastDiscoveryDate": 1749446451563,
"firstDiscoveryDateStr": null,
"lastBeforeDiscoveryDateStr": null,
"validFor": "364 day(s) 18 hr(s) 52 min(s)",
"keyAlgorithmAndSize": "RSA 2048",
"signatureAlgorithm": "SHA256withRSA",
"signatureHashAlgorithm": null,
"keyUsage": "DigitalSignature, KeyEncipherment",
"extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) ",
"basicConstraints": "Subject Type=End entity, Path Length=none",
"group": null,
"subjectAlternativeNames": [
    "DNS : pe-cert-swat-n12.lab.appviewx.net"
],
"complianceStatus": "",
"applications": [
    "192.168.220.120:10250"
],
"policyIdentifiers": [],
"expiryStatus": "Valid",
"permission": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"category": "Server",
"uuid": "7553cccc7a03ef070e5fb22132bd885433335ec7",
"id": null,
"certificateAuthority": "OTHERS",
"authorityKeyIdentifier": "BF:DD:9E:7F:86:30:9F:9C:8D:05:5C:CB:33:4B:9B:65:14:71:23:A6",
"subjectKeyIdentifier": "",
"issuerSerialNumber": null,
"authorityInfoAccess": [],
"certificatePolicies": [],
"crlDistributionPoints": [],
"thumbprintAlgorithm": null,
"thumbPrint": "C2:85:2C:5A:1B:F3:F5:1B:FF:17:B7:43:84:DA:64:4B:8E:50:3C:2E",
"type": "Others",
"genericFields": null,
"certAttributes": null,
"customAttributes": null,
"validFromDate": null,
"validToDate": null,
"discoveredFileNames": [],
"issuingTemplate": null,
"csrGenerationSource": null,
"certificateHSMDetails": null,
"deviceDetails": null,
"newConnectors": [
    "192.168.220.120:10250:absecon"
],
"csrAvailable": false,
"enhancedSANTypes": null,
"autoRenewDate": null,
"autoRegenDate": null,
"missingParamsForAutoRenew": null,
"base64ImageContent": null,
"caConnectorName": null,
"caSettingName": null,
"suspendedCertificate": false,
"comments": null,
"mailAddress": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "streetAddress": null,
            "postalCode": null,
            "publicKeyModulus": null,
            "requestIds": null,
            "orderId": null,
            "publicKey":
 "30:82:01:0A:02:82:01:01:00:B0:B6:FB:AF:F0:96:B5:19:0C:B5:3E:4B:F3:73:0A:A0:15:3E:5F:69:05:CB:23:75:2A:3B:2E:DF:B2:55:10:5D:2E:AB:6F:43:D7:6B:12:3
C:03:B3:F8:D7:0F:F1:54:3A:7A:38:2D:F6:66:CA:45:F4:91:FD:0B:A4:4B:B3:E5:48:F5:99:35:28:52:68:11:93:02:44:82:03:46:74:BF:AB:1B:F1:64:B5:01:82:7C:AC:
C4:D7:3E:8F:7B:CB:C1:A8:C4:21:BA:E5:90:3A:89:20:B6:E1:9B:60:C3:2F:98:42:18:70:AB:78:6F:9E:AD:09:95:DE:EC:18:1B:74:72:4F:F8:32:45:B8:4C:C6:9B:12:
DD:DD:CA:8F:4E:22:A2:52:E6:AC:96:D5:6E:85:08:F0:DA:44:DD:4E:DA:A5:9D:C1:91:45:1A:D0:DC:91:90:9B:51:9C:74:FB:F6:EE:55:EE:41:F1:57:FD:3A:72:B7:9
2:AB:F6:D5:02:88:E9:69:4F:E3:38:E3:FB:8B:67:5E:06:2B:D6:33:C4:FE:5D:5E:BD:E3:6C:8D:0F:BA:1D:5D:09:55:E2:23:EF:46:DF:8A:8B:F1:D6:7B:34:00:56:52:C
5:63:E9:A7:E2:48:58:D3:D9:B7:C9:BC:0E:B9:EF:BE:1E:A4:24:90:0F:E2:E5:2E:87:02:03:01:00:01",
            "ellipticCurve": null,
            "issuedByRootCertificate": false,
            "cumulativeSanCount": 1,
            "chainPriority": 0,
            "caCertificateType": null,
            "templateProfile": null,
            "certificateTags": null,
            "resourceTags": null,
            "ocspStatus": null,
            "enrollmentMethod": null,
            "kubeService": null,
            "subject": "CN=pe-cert-swat-n12.lab.appviewx.net@1749432603",
            "discoveryTypes": null,
            "certLifeCycleAction": null,
            "certLifeCycleActionTimestamp": 0,
            "isSsoActive": null,
            "customExtensions": null,
            "privatekeyAvaliable": false,
            "cvss": null
        },
        {
            "commonName": "appviewx.onpremise.com",
            "serialNumber": "4E:00:31:6D:38:BA:CF:4A:D9:20:41:B0:2C:6B:01:BF",
            "serialNumberHex": "4e00316d38bacf4ad92041b02c6b01bf",
            "issuerCommonName": "appviewx.onpremise.com",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"status": null,
"avxStatus": "Discovered",
"associatedObjects": [],
"discoverySources": [
    "pe-cert-swat-120.lab.appviewx.net:31443"
],
"subjectOrganization": "",
"subjectOrganizationUnit": "",
"subjectLocality": "",
"subjectState": "",
"subjectCountry": "",
"issuerOrganization": "",
"issuerOrganizationUnit": "",
"issuerLocality": "",
"issuerState": "",
"issuerCountry": "",
"version": "3",
"validFrom": 1749432506000,
"validTo": 2064792506000,
"firstDiscoveryDate": 1749446451563,
"lastBeforeDiscoveryDate": 1749446451563,
"lastDiscoveryDate": 1749446451563,
"firstDiscoveryDateStr": null,
"lastBeforeDiscoveryDateStr": null,
"validFor": "3649 day(s) 19 hr(s) 51 min(s)",
"keyAlgorithmAndSize": "RSA 2048",
"signatureAlgorithm": "SHA256withRSA",
"signatureHashAlgorithm": null,
"keyUsage": "DigitalSignature, KeyEncipherment",
"extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2) ",
"basicConstraints": "Subject Type=End entity, Path Length=none",
"group": null,
"subjectAlternativeNames": [],
"complianceStatus": "",
"applications": [
    "192.168.220.120:31443"
],
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"policyIdentifiers": [],
"expiryStatus": "Valid",
"permission": null,
"category": "Server",
"uuid": "ed9d0ee0ef80c3f914627e712bd586bb3c818114",
"id": null,
"certificateAuthority": "OTHERS",
"authorityKeyIdentifier": "",
"subjectKeyIdentifier": "",
"issuerSerialNumber": null,
"authorityInfoAccess": [],
"certificatePolicies": [],
"crlDistributionPoints": [],
"thumbprintAlgorithm": null,
"thumbPrint": "1B:68:CF:26:DA:59:1A:7B:AD:DA:79:33:61:27:25:5E:F9:73:B7:53",
"type": "Self Signed",
"genericFields": null,
"certAttributes": null,
"customAttributes": null,
"validFromDate": null,
"validToDate": null,
"discoveredFileNames": [],
"issuingTemplate": null,
"csrGenerationSource": null,
"certificateHSMDetails": null,
"deviceDetails": null,
"newConnectors": [
    "192.168.220.120:31443:absecon"
],
"csrAvailable": false,
"enhancedSANTypes": null,
"autoRenewDate": null,
"autoRegenDate": null,
"missingParamsForAutoRenew": null,
"base64ImageContent": null,
"caConnectorName": null,
"caSettingName": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "suspendedCertificate": false,
            "comments": null,
            "mailAddress": "",
            "streetAddress": null,
            "postalCode": null,
            "publicKeyModulus": null,
            "requestIds": null,
            "orderId": null,
            "publicKey":
 "30:82:01:0A:02:82:01:01:00:EF:4C:46:3B:34:C6:41:97:77:36:C3:BA:FA:0F:8A:2B:A8:C6:3A:8F:7E:E1:E9:83:BD:C0:58:B5:66:29:E5:3A:5D:9D:3F:0E:B8:8D:E8:
4D:CC:D2:64:04:6D:6D:D1:2F:17:60:DC:AC:7D:BF:85:05:17:4F:05:06:51:8F:8C:22:48:1F:49:20:F0:4C:15:40:E4:1E:83:17:C0:E6:69:AE:36:FC:7C:55:2D:E0:59:E
8:3F:63:51:60:17:B1:C8:0B:55:1D:82:E9:FB:28:E4:45:88:8F:CA:8E:95:85:52:79:C8:93:B5:F5:31:03:1B:36:FA:B8:CF:05:4A:D8:0E:06:EE:10:FC:64:7E:4C:E4:A6:
B0:24:A1:7A:DF:D7:3A:45:E5:DE:2A:0D:3B:AE:A1:BE:F5:C4:41:D6:43:4A:8B:2C:86:9C:DF:AD:CD:82:1A:D6:58:59:9D:9C:2F:D8:78:17:51:02:74:FA:0A:88:1B:0
4:B9:DE:93:02:FB:08:E8:57:6B:C4:F7:1C:71:DA:50:1D:26:25:57:26:9E:0C:B6:F8:BD:73:6F:31:86:99:12:74:E9:6C:1B:E1:09:D8:7D:19:CF:CF:15:5A:F6:AE:35:B0
:44:4F:E7:1E:35:8A:A7:D6:66:5D:3B:FA:8B:B4:74:51:E8:8A:21:1C:44:79:87:D5:02:03:01:00:01",
            "ellipticCurve": null,
            "issuedByRootCertificate": false,
            "cumulativeSanCount": 0,
            "chainPriority": 0,
            "caCertificateType": null,
            "templateProfile": null,
            "certificateTags": null,
            "resourceTags": null,
            "ocspStatus": null,
            "enrollmentMethod": null,
            "kubeService": null,
            "subject": "CN=appviewx.onpremise.com",
            "discoveryTypes": null,
            "certLifeCycleAction": null,
            "certLifeCycleActionTimestamp": 0,
            "isSsoActive": null,
            "customExtensions": null,
            "privatekeyAvaliable": false,
            "cvss": null
        }
    ],
    "autoSuggest": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "executionTime": 1749447433,
    "iTotalDisplayRecords": 6
  },
  "message": null,
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fetch Devices Discovered During a Network Scan

The API enables users to fetch the discovered devices from a particular discovery instance (Network Scan) using the discovery name.

Before you begin

- The user should have the ACF permission to view the certificate discovery.

Request Structure

Endpoint:	/certificate/discovery/devicesList
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/devicesList?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String
userName *Header*	(Mandatory) Username for logging in to AppViewX. **Type**: String
password *Header*	(Mandatory) Password for logging in to AppViewX. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload*Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
name	(Mandatory) Name of the discovery instance created. **Type**: String
searchTextValue	(Optional) Query the fetched results based on the provided search value.
sortColumn	(Optional) specifies the column on which the sort has to be applied.
sortOrder	(Optional) specifies the sort order to be applied. **Constraint:** Possible values : 1, -1, asc, desc
maxSize	(Optional) specifies the maximum number of results that can be retrieved. **Constraint :** Possible values in the range 1 to 100.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes. **Type:** A JSON object

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
search	null
totalRecords	Total number of records in the specified discoveryInstance.
data	Device metadata. **Type**: Array of Device Data json
autoSuggest	null
executionTime	Execution time of the request.
iTotalDisplayRecords	Total number of records in the specified discoveryInstance.
message	If matching records are found for the search query - null. If no records are available for the search query - No matching records found. **Type:** String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type:** String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Response contains the device data of the specified discovery instance.
400 Bad Request	INVALID_REQUEST	Invalid request specified - <reason>. **Remediation**: Ensure that the payload/query param is valid and the <reason> is handled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password is provided as header parameters.
403 Forbidden	AVX_GW_005	The user does not have view permission to the Discovery.
404 Not Found	MSG_DISC_DISCOVERY_NAME_NOTFOUND	Discovery name: <Discovery Name> not available. **Remediation**: Check whether the discoveryName provided is valid and is present.
407 Proxy Authentication Required	AVX_GW_011	Session validation failed, reason - Session information is missing. **Remediation**: Ensure the headers are correctly mentioned with correct authentication information.
500 Internal Server Error	MSG_DISC_DISCOVERY_NAME_NULLOREMPTY	Discovery name: Null or Empty. **Remediation**: Ensure the discoveryName parameter is not empty or null in the payload/query param.

Sample Request/Response

Request Payload

```
{
  "searchTextValue": "",
  "startIndex": 0,
  "sortColumn": "ip",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "sortOrder": "asc",
  "name": "Test Discovery",
  "maxSize": 1
}
```


Response


```
{
  "response": {
    "search": null,
    "totalRecords": 245,
    "data": [
      {
        "ip": "192.168.145.105",
        "hostname": "pfiu-sdet-f5-n1.lab.appviewx.net",
        "latency": "0.0017s",
        "networkDistance": "3 hops",
        "scanTime": "14.29 seconds",
        "deviceType": "load balancer",
        "discoveryId": "685564cda69dcc148066cfef",
        "batchNumber": 2,
        "port": "443",
        "vendor": "F5, Apache",
        "os": "Linux 4.0 - 4.4",
        "version": "Apache httpd (F5 BIG-IP load balancer)",
        "_id": "192.168.145.105#443#685564cda69dcc148066cfef"
      }
    ],
    "autoSuggest": null,
    "executionTime": 1750675007,
    "iTotalDisplayRecords": 245
  },
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Fetch Cipher–TLS Version Mapping from Discovery Execution

The API enables users to fetch cipher–TLS version mappings for each discovery execution, along with metadata such as discovery execution ID, start and end times, and target endpoints. This is applicable for Discovery Types, IPRANGE, SUBNET, and NETWORK.

Before you begin

- The user should have `DISCOVERY_CREATE_EDIT` as ACF permission.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/discovery/instance?discoveryName=<name>
Type:	GET
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/instance?discoveryName=<name>&gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Header*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
discoveryName*Header*	(Mandatory) Name of the discovery instance. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
skip*Header*	(Optional) skip is from which the response has to be available. For example, if the response has to skip the first 100 and show the next 50, then the start index has to be 101. **Type**: Integer **Constraint**: Default value is 0.
limit*Header*	(Optional) The number of entries from the start index to be made available. For example, if the response is expected to have skipped the first 100 and show the next 50, then the start index has to be 101 and max has to be 50. **Type**: Integer **Constraint**: Default value is 100 and max value is 100.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes. **Type:** A JSON object
vulnerabilityRecords	Vulnerability Records. **Type:** Array
columnHeader	null
data	Certificate metadata. **Type**: Array of Certificate json String
totalRecords	Total Number Records available for this discovery. Help while doing pagination until you fetch all records.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
executionTime	Execution time of the request.
iTotalDisplayRecords	Total number of records in the specified discoveryInstance.
headers	null
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type:** String
tags	null
response	Contains the response attributes. **Type**: JSON object
vulnerabilityRecords	List of vulnerability records for each scanned IP/port. **Type**: Array
ip	IP address of the scanned endpoint. **Type**: String
port	Port number used for scanning. **Type**: Integer
cipherSuites	Map of cipher names with their strength levels, with ::TLS version suffix. **Type**: Object
sslCiphers	List of individual cipher objects. **Type**: Array
name	Name of the cipher suite. **Type**: String
strength	Security strength classification (for example, HIGH, UNKNOWN).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
protocolVersion	TLS protocol version (for example, TLSv1.2, TLSv1.3). **Type**: String
tlsSslVersions	TLS versions and their overall security rating. **Type**: Object
cipherFetchStatus	Status of the cipher fetching operation. **Type**: String
hostName	Resolved hostname (if available). **Type**: String or null
group	null
certificateUuid	null
message	Any messages returned for the endpoint. **Type**: Array of Strings
cvss	null
columnHeader	null
totalRecords	Total number of vulnerability records available for this discovery. Useful for pagination. **Type**: Integer
executionTime	Time taken to execute the request.
iTotalDisplayRecords	Total number of vulnerability records available for this discovery. Useful for pagination. **Type**: Integer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
discoveryEndTime	End Time of Discovery in GMT. **Type**: String
headers	null
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Metadata or upstream error tags. **Type**: Object
message	Error message (if any). **Type**: String or null

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Accepted.
400 Bad Request	ERR_DISC_DISCOVERY_HISTORY_RETRIVAL	Error while retrieving discovery history. **Remediation**: Discovery name passed in the request should be present in the database.
400 Bad Request	NO_RECORDS_FOUND	No matching records found. **Remediation**: Discovery name passed in the request should be present in the system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	MANDATORY_QUERY_PARAM_MISSING	Mandatory query param is missing or invalid. **Remediation**: The parameter <discoveryName> must be present in the URL request.
417 Expectation failed	CERT-FV-001	Invalid query param found for discoveryName. **Remediation**: The discoveryName value should be a minimum of 2 characters.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload

https://%3CIP/HostName/TenantName%3E:%3CGWPORT%3E/avxapi/certificate/discovery/reports/ciphers?discoveryName=testScan&gwkey=f000ca01&gwsource=external&limit=100&skip=0

Response


```
{
  "response": {
    "vulnerabilityRecords": [
      {
        "certificateUuid": null,
        "ip": "192.168.224.5",
        "port": 443,
        "cipherSuites": {
          "TLS_AKE_WITH_AES_128_GCM_SHA256::TLSv1.3": "UNKNOWN",
          "TLS_AKE_WITH_AES_256_GCM_SHA384::TLSv1.3": "UNKNOWN",
          "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256::TLSv1.2": "HIGH",
          "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256::TLSv1.2": "HIGH",
          "TLS_AKE_WITH_CHACHA20_POLY1305_SHA256::TLSv1.3": "UNKNOWN",
          "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384::TLSv1.2": "HIGH"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    },
    "sslCiphers": [
        {
            "name": "TLS_AKE_WITH_AES_128_GCM_SHA256",
            "strength": "UNKNOWN",
            "protocolVersion": "TLSv1.3"
        },
        {
            "name": "TLS_AKE_WITH_AES_256_GCM_SHA384",
            "strength": "UNKNOWN",
            "protocolVersion": "TLSv1.3"
        },
        {
            "name": "TLS_AKE_WITH_CHACHA20_POLY1305_SHA256",
            "strength": "UNKNOWN",
            "protocolVersion": "TLSv1.3"
        },
        {
            "name": "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "strength": "HIGH",
            "protocolVersion": "TLSv1.2"
        },
        {
            "name": "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "strength": "HIGH",
            "protocolVersion": "TLSv1.2"
        },
        {
            "name": "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
            "strength": "HIGH",
            "protocolVersion": "TLSv1.2"
        }
    ],
    "hostName": null,
    "group": null,
    "tlsSslVersions": {
        "TLSv1.3": "HIGH",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                "TLSv1.2": "HIGH"
            },
            "cipherFetchStatus": "Success",
            "message": [],
            "cvss": null
        }
    ],
    "columnHeader": null,
    "totalRecords": 1,
    "executionTime": 15,
    "iTotalDisplayRecords": 1,
    "discoveryStartTime": "06/17/25 07:24:16",
    "discoveryEndTime": "06/17/25 07:34:09"
  },
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Delete Certificate Discovery

This API is used to delete discoveries.

Request Structure

Endpoint:	/cert-discovery-history-delete
Type:	PUT
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/cert-discovery-history-delete?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId	(Mandatory) Session ID received after login.
Header	**Type**: String
	Constraints: Required if **username** and **password** are not provided.
userName	(Mandatory) Username that is configured in AppViewX.
Header	**Type**: String
password	(Mandatory) Password of that user.
Header	**Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload (Refer **Payload** table below)

Payload

Payload

Name	Description
NA	(Mandatory) Discovery IDs **Type**: Array of String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the enrollment request.
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Success.
400 Bad Request	AVX-VLDTN-001	Invalid payload data. **Remediation**: Ensure the payload is correct or meets the validation rules specified by the validation protocol.
400 Bad Request	MSG_DISC_DISCOVERY_NOTFOUND	Discovery details not available. **Remediation**: The discovery ID must be valid or present in the database.
500 Internal Server Error	avx-common-011	Error while processing.

Sample Request/Response

Request Payload

```
["507f1f77bcf86cd799439011", "507f1f77bcf86cd799439022", "507f1f77bcf86cd799439033"]
```

Response

```
{
"response": "success",
"message": null,
"appStatusCode": null,
"tags": null
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Upload Multiple Certificates to the Inventory

This API is used to upload multiple certificates to the AppViewX certificate inventory in a single upload operation.

Before you begin

- The user should have the ACF permission to create/edit/rediscover/replay under certificate discovery.
- The certificate group name that will be specified in the payload should have RW permissions.
- The discovery name should be unique.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	certificate/discovery/upload
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/discovery/upload?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
userName *Header*	(Mandatory) Username that is configured in AppViewX. **Type**: String
password *Header*	(Mandatory) Password of that user. **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *payload*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload (Refer **Payload** table below)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
discoveryName	(Mandatory) Name of the discovery instance. **Type**: String
certificateCategory	(Optional) Certificate category **Type**: String **Possible Values**: Server, Client, Code Signing, Server and Client, Device, Root, Intermediate, Others
groupName	(Mandatory) Name of the group to which the certificate belongs. **Type**: String
status	(Optional) Status indicating whether the certificate is managed or monitored. **Type**: String **Possible Values**: Managed, Monitored
uploadContent	(Mandatory) Details of the certificate to be uploaded. **Type**: uploadContent

uploadContent Parameters

Name	Description
fileContent	(Mandatory) Content of the file in byte array format for the certificate to be uploaded. **Type:** byte array
fileName	(Mandatory) Name of the file. **Type:** String
password	(Optional) Password associated with the file (depending on the file type).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

uploadContent Parameters (continued)

Name	Description
	Type: String
keyToDecrypt	(Optional) Key to decrypt the password if it is encrypted. **Type:** String
certID	(Mandatory) Certificate ID. **Type:** String
woID	(Mandatory) Work order ID (to be sent at NA). **Type:** String
certificateCategory	(Optional) Category of the certificate. **Type:** String
certificateAuthority	(Optional) Certificate Authority **Type:** String
comments	(Optional) Additional comments. **Type:** String
groupName	(Optional) Name of the group to which the certificate belongs. **Type:** String
proxyRequired	(Optional) Determines if a proxy is required. **Type:** Boolean (true/false)
dataCenter	(Optional) Name of the datacenter where the API is to be executed. **Type:** String
caId	(Optional) Certificate authority ID. **Type:** String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

uploadContent Parameters (continued)

Name	Description
avxStatus	(Optional) Status indicating whether the certificate is managed or monitored. **Type:** String **Possible values:** Managed, Monitored
enrollmentMethod	(Optional) Method used for certificate enrollment. **Type:** String **Possible Values:** SCEP, EST, ACME, SCEP_MS_INTUNE, MS_PROXY/WAEP
kubeService	(Optional) Name of the Kubernetes service. **Type:** String **Possible Values:** cert-orchestrator, appviewx-signer, appviewx-infra-orchestrator, appviewx-csi-provider
metadata	(Optional) A key-value pair of metadata info. **Type:** Map<String,Object>
isValid	(Optional) Determines if the certificate is valid. **Type:** Boolean (true/false)
encodedPassword	(Optional) The base-64 encoded password value. **Type:** String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: response
message	Displays the number of records found if success or a failure message. **Type:** String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type:** String
tags	Additional information in case of failure response.
headers	HTTP headers associated with the response. **Type:** String

response

Name	Description
discoverId	ID assigned to the discovery instance **Type:** response

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	Accepted.
400 Bad Request	AVX-VLDTN-001	Invalid payload data. **Remediation**: Ensure the payload is correct or meets the validation rules specified by the validation protocol.
400 Bad Request	INVALID_GROUP_NAME	groupName is Invalid or the user does not have enough permission for the specified group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: The group name should be valid and have the required permissions.
400 Bad Request	MSG_DISC_HISTORY_UNIQUE_NAME	Discovery name already exists. Please specify different Discovery name. **Remediation**: The discovery name should be unique.
500 Internal Server Error	avx-common-011	Internal Server Error.

Sample Request/Response

Request Payload

```
{
 "discoveryName": "<name>",
 "certificateCategory": "<ROOT_CA/INTERMEDIATE_CA/SERVER/CLIENT/SERVER_AND_CLIENT/CODE_SIGNING/DEVICE/OTHERS>",
 "groupName": "<name>",
 "status": "<>",
 "uploadContent": {
  "fileContent": <byte[]>,
  "fileName": "<name>",
  "password": "",
  "keyToDecrypt": "",
  "certId": "<>",
  "woId": "<NA>",
  "certificateCategory": "",
  "certificateAuthority": "",
  "comments": "",
  "groupName": "",
  "proxyRequired": true/false,
  "dataCenter": "",
  "caId": "",
  "avxStatus": "Managed/Monitored",
  "enrollmentMethod": "SCEP/EST/ACME/SCEP_MS_INTUNE/MS_PROXY/WAEP",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 "kubeService": "cert-orchestrator/ appviewx-signer/ appviewx-infra-orchestrator/ appviewx-csi-provider",
 "metadata": {


 },
 "isValid": true/false,
 "encodedPassword": ""
},
"uploadContents": [ --> max of 5000 entries to be sent in uploadContents
 {<similar object as uploadContent field>},
 {<similar object as uploadContent field>}
],
"comments": ""
}
```

Response

```
{
 "response": {
   "discoverId": "507f1f77bcf86cd799439011"
 },
 "message": "Discovery Request is created successfully - 507f1f77bcf86cd799439011",
 "appStatusCode": null,
 "tags": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Upload Server Certificate to the Inventory

This API is used to upload a single server certificate to the AppViewX server certificate inventory.

Before you begin

- The user has the ACF permission to upload a certificate within the uploaded certificate's category.

Request Structure

Endpoint:	/cert-upload-server-certificate
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/cert-upload-server-certificate?gwsource=external` To understand the elements of the sample URL, click here.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
username	(Mandatory) Username that is configured in AppViewX.
Header	**Type**: String
password	(Mandatory) Password of that user.
Header	**Type**: String
content-type	(Mandatory) Payload content-type with application/json value.
Header	**Type**: String
	Constraint: The value must be **application/json**.
gwsource	(Mandatory) The source from which the request is triggered, e.g., external.
Query	**Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request.
payload	**Type**: Payload (Refer **Payload** table below)

Payload

Payload

Name	Description
groupName	(Optional) Group associated with the certificate.
	Type: String
fileName	(Mandatory) Name of the certificate file that has to be uploaded.
	Type: String
fileContent	(Mandatory) Certificate file data encoded and uploaded as a raw binary stream.
	Type: byte[]
certificateCategory	(Optional) Certificate category.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Possible values**: Server **Constraints**: Parameter value cannot be **CA**.
wold	(Mandatory) ID of the work order for the upload request. **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Error Response Parameters

Name	Description
response	Contains the response attributes.
message	Success message of the action or failure description in case of an error. **Type:** String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type:** String
tags	Additional information in case of failure response.

Name	Description
message	Success message or failure description in case of error. **Type:** String
uuid	Uuid of the uploaded certificate. **Type:** String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Description
commonName	Common name of the uploaded certificate. **Type:** String
category	Category of the uploaded certificate. **Type:** String
id	Unique identifier of the certificate. **Type:** String
avxStatus	Status of the certificate in Appviewx. (Managed, Monitored, Discovered) **Type:** String

Status Codes

HTTP Code	appStatusCode	Response Message
200 Success	NA	Certificate uploaded successfully.
400 Bad Request	VALIDATION_ERROR_0004	Mandatory field is missing or invalid - value. **Remediation**: Ensure that the mandatory field specified in the error message is present in the payload and has the accepted value.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameter.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure that the given user has the proper ACF permissions to upload a certificate.
500 Internal Server Error	avx-common-011	Internal Server Error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload

```
{
   "payload": {
     "groupName": "Default",
     "fileName": "testAlbpushBind.appviewx.com.crt",
     "fileContent": (base64-encoded certificate content),
     "certificateCategory": "server",
     "woId": "NA"
   }
 }
```

Response

```
{
  "response": {
    "uuid": "977f0f2acf5c3613b16034298a20ed04d36b9df6",
    "message": "Certificate has been uploaded successfully.",
    "commonName": "testAlbpushBind.appviewx.com",
    "category": "Server",
    "id": "68396eeb4533c80d36219cda",
    "avxStatus": "Managed"
  }
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

View a Certificate Group

This API is used to view the configuration details of a certificate group.

Before you Begin

- The user should have the required ACF permissions to view the certificate group.

Request Structure

Endpoint:	/certificate/group
Type:	GET
Action:	certificate-group-view
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?groupName=<groupName>&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
groupName *Header*	(Mandatory) Name of the certificate group whose details have to be retrieved
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

response

Name	Description
name	Name of the group who details have been retrieved **Type**: String
displayName	Display name configured for the group **Type**: String
description	Description of the certificate group **Type**: String
applicationID	Organization ID associated with the group **Type**: String
policyName	Certificate policy associated with the group **Type**: String
groupBusinessInfo	Details of the business unit associated with the group **Type**: groupBusinessInfo

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

response (continued)

Name	Description
groupLevelCertConfig	Configuration details for the certificates associated with this group **Type**: groupLevelCertConfig

groupBusinessInfo

Name	Description
contactName	Contact of the associated business unit's contact person
firstName	First name of the associated business unit's contact person
lastName	Last name of the associated business unit's contact person
phoneNumber	Phone number of the associated business unit's contact person
lobName	Name of the business unit associated with the certificate group
costCenter	Code/label of the cost center associated with the certificate group
environmentName	Business unit environment associated with the certificate group
inventoryNumber	Inventory tracking number for the certificate group
email	Email address of the associated business unit's contact person

groupLevelCertConfig

Name	Description
autoPushFlag	Indicates whether certificates assigned to this group will be automatically pushed to the target endpoint upon renewal/regeneration
groupOverrideFlag	Indicates if the group level settings for auto renewal/regeneration will override the certificate level settings
connectorStatusToSkip	Indicates if application connector cloning (after certificate renewal, regeneration, and resissue) is enabled
autoRenewConfig	Indicates the auto renewal-related configuration details for this certificate group **Type**: autoRenewConfig
autoRegenerateConfig	Indicates the auto regeneration-related configuration details for this certificate group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

groupLevelCertConfig (continued)

Name	Description
	Type: autoRegenerateConfig
parentGroup	Name of the parent certificate group under which the new certificate group is created
deleteRestricted	Indicates if this certificate group can be deleted
_id	Unique identifier assigned to the certificate group

autoRenewConfig

Name	Description
renewBefore	For the certificates associated with this group, indicates how many days prior to a certificate's expiry the renewal process will start
autoRenewalFlag	Indicates if auto renewal is enabled for the certificates associated with this group
approvalRequiredFlag	Indicates if approval is required before certificate renewal is triggered

autoRegenerateConfig

Name	Description
regenerateBefore	For the certificates associated with this group, indicates how many days prior to a certificate's expiry the regeneration process will start
autoRegenerateFlag	Indicates if auto regeneration is enabled for the certificates associated with this group
approvalRequiredFlag	Indicates if approval is required before certificate regeneration is triggered

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Deletion action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
404 Not Found	CERT-GRP-0003	Group information not available **Remediation**: Ensure that the group information provided in the request is correct. If the issue still persists, contact AppViewX support.
500 Internal server error	CERT-GRP-0005	Error occurred while fetching the certificate group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Contact AppViewX support.

Sample Request/Response

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?groupName=MasterGroup1&gwsource=external
```

Sample Response


```
{
  "response": [
    "Private_CA_Certificates",
    "Public_CA_Certificates",
    "MasterGroup",
    "Certificate-Gateway",
    "Default",
    "MasterGroup11",
    "MasterGroup10"
  ],
  "message": "7 record(s) found",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Create a Certificate Group

This API is used to create a certificate group. Certificate groups are logical containers used for organizing, managing, and applying bulk actions to certificates efficiently.

Before you Begin

- The user should have the required ACF permissions to create the certificate group.

Request Structure

Endpoint:	/certificate/group
Type:	POST
Action:	certificate-group-create
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
name	(Mandatory) Name for the new certificate group **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
displayName	(Optional) Display name for the new certificate group **Type**: String
description	(Optional) Additional details related to the new certificate group **Type**: String
applicationID	(Optional) Organization ID that must be associated with the new group **Type**: String
parentGroup	(Optional) Name of the parent certificate group under which the new certificate group will be created **Type**: String
policyName	(Mandatory) Certificate policy that must be associated with the new group **Type**: String
groupBusinessInfo	(Optional) Details of the business unit that must be associated with the new group **Type**: groupBusinessInfo
groupLevelCertConfig	(Optional) Configuration details for the certificates that will be associated with this group **Type**: groupLevelCertConfig

groupBusinessInfo

Name	Description
contactName	(Optional) Contact of the associated business unit's contact person **Type**: String
firstName	(Optional) First name of the associated business unit's contact person

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

groupBusinessInfo (continued)

Name	Description
	Type: String
lastName	(Optional) Last name of the associated business unit's contact person **Type**: String
phoneNumber	(Optional) Phone number of the associated business unit's contact person **Type**: String
lobName	(Optional) Name of the business unit associated with the certificate group **Type**: String
costCenter	(Optional) Code/label of the cost center associated with the certificate group **Type**: String
environmentName	(Optional) Business unit environment associated with the certificate group **Type**: String
inventoryNumber	(Optional) Inventory tracking number for the certificate group **Type**: String
email	(Optional) Email address of the associated business unit's contact person **Type**: String

groupLevelCertConfig

Name	Description
autoPushFlag	(Optional) Specify if certificates assigned to this group will be automatically pushed to the target endpoint upon renewal/regeneration **Type**: Boolean
groupOverrideFlag	(Optional) Specify if the group level settings for auto renewal/regeneration will override the certificate level settings

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

groupLevelCertConfig (continued)

Name	Description
	Type: Boolean
autoRenewConfig	(Optional) Specify the auto renewal-related configuration details for this certificate group **Type**: autoRenewConfig
autoRegenerateConfig	(Optional) Specify the auto regeneration-related configuration details for this certificate group **Type**: autoRegenerateConfig

autoRenewConfig

Name	Description
renewBefore	(Mandatory if **autoRenewalFlag** is enabled) For the certificates associated with this group, indicates how many days prior to a certificate's expiry the renewal process will start **Type**: Integer
autoRenewalFlag	(optional) Specify if auto renewal must be enabled for the certificates associated with this group **Type**: Boolean
approvalRequiredFlag	(Optional) Indicates if approval is required before certificate renewal is triggered **Type**: Boolean

autoRegenerateConfig

Name	Description
regenerateBefore	(Mandatory if **autoRegenerateFlag** is enabled) For the certificates associated with this group, indicates how many days prior to a certificate's expiry the regeneration process will start

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

autoRegenerateConfig (continued)

Name	Description
	Type: Integer
autoRegenerateFlag	(optional) Specify if auto regeneration must be enabled for the certificates associated with this group **Type**: Boolean
approvalRequiredFlag	(Optional) Indicates if approval is required before certificate regeneration is triggered **Type**: Boolean

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response for the group creation operation **Type**: Boolean
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Reissue action has been triggered successfully

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason: Invalid credentials **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
400 Bad Request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
  "name": "MasterNewGroup",
  "displayName": "",
  "description": "",
  "applicationId": "1",
  "parentGroup": "Default",
  "policyName": "Default",
  "groupBusinessInfo": {
      "contactName": "",
      "phoneNumber": "",
      "firstName": "",
      "lastName": "",
      "lobName": "",
      "costCenter": "",
      "environmentName": "",
      "inventoryNumber": "",
      "email": ""
  },
  "groupLevelCertConfig": {
      "autoPushFlag": false,
      "groupOverrideFlag": false,
      "autoRenewConfig": {
          "renewBefore": 0,
          "autoRenewalFlag": false,
          "approvalRequiredFlag": false
      },
      "autoRegenerateConfig": {
          "regenerateBefore": 0,
          "autoRegenerateFlag": false,
          "approvalRequiredFlag": false
      }
  }
}
```


Sample Response


```
{
  "response": true,
  "message": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Update a Certificate Group

This API is used to modify the configuration of an existing certificate group.

Before you Begin

- The user should have the required ACF permissions to modify the certificate group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/group
Type:	PUT
Action:	certificate-group-update
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
name	(Mandatory) Name of the certificate group to be updated **Type**: String
displayName	(Optional) Display name assigned to the certificate group **Type**: String
description	(Optional) Additional details related to the certificate group **Type**: String
applicationID	(Optional) Organization ID that associated with the certificate group **Type**: String
parentGroup	(Optional) Name of the parent certificate group associated with the certificate group that is to be updated **Type**: String
policyName	(Mandatory) Certificate policy associated with the group **Type**: String
groupBusinessInfo	(Optional) Details of the business unit associated with the group **Type**: groupBusinessInfo
groupLevelCertConfig	(Optional) Configuration details for the certificates associated with the group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: groupLevelCertConfig

groupBusinessInfo

Name	Description
contactName	(Optional) Contact of the associated business unit's contact person **Type**: String
firstName	(Optional) First name of the associated business unit's contact person **Type**: String
lastName	(Optional) Last name of the associated business unit's contact person **Type**: String
phoneNumber	(Optional) Phone number of the associated business unit's contact person **Type**: String
lobName	(Optional) Name of the business unit associated with the certificate group **Type**: String
costCenter	(Optional) Code/label of the cost center associated with the certificate group **Type**: String
environmentName	(Optional) Business unit environment associated with the certificate group **Type**: String
inventoryNumber	(Optional) Inventory tracking number for the certificate group **Type**: String
email	(Optional) Email address of the associated business unit's contact person **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

groupLevelCertConfig

Name	Description
autoPushFlag	(Optional) Specify if certificates assigned to this group will be automatically pushed to the target endpoint upon renewal/regeneration **Type**: Boolean
groupOverrideFlag	(Optional) Specify if the group level settings for auto renewal/regeneration will override the certificate level settings **Type**: Boolean
autoRenewConfig	(Optional) Specify the auto renewal-related configuration details for this certificate group **Type**: autoRenewConfig
autoRegenerateConfig	(Optional) Specify the auto regeneration-related configuration details for this certificate group **Type**: autoRegenerateConfig

autoRenewConfig

Name	Description
renewBefore	(Mandatory if **autoRenewalFlag** is enabled) For the certificates associated with this group, indicates how many days prior to a certificate's expiry the renewal process will start **Type**: Integer
autoRenewalFlag	(optional) Specify if auto renewal must be enabled for the certificates associated with this group **Type**: Boolean
approvalRequiredFlag	(Optional) Indicates if approval is required before certificate renewal is triggered **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

autoRegenerateConfig

Name	Description
regenerateBefore	(Mandatory if **autoRegenerateFlag** is enabled) For the certificates associated with this group, indicates how many days prior to a certificate's expiry the regeneration process will start **Type**: Integer
autoRegenerateFlag	(optional) Specify if auto regeneration must be enabled for the certificates associated with this group **Type**: Boolean
approvalRequiredFlag	(Optional) Indicates if approval is required before certificate regeneration is triggered **Type**: Boolean

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response for the group update operation **Type**: Boolean
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Update action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId. **Remediation**: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
417 Expectation failed	CERT-GRP-0001	Group already exists with the given name **Remediation**: Ensure that the group name is unique and not a duplicate of an existing group.
417 Expectation failed	CERT-GRP-0010	Default group can be associated with the default policy only

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: For the default group, set **policyName** to the default policy only.
417 Expectation failed	CERT_0010	Parent name and group name cannot be the same. **Remediation**: Correct the updated group name.
400 Bad request	CERT-PLCY-0009	Policy name is invalid. **Remediation**: Ensure that the policy name is valid.

Sample Request/Response

Sample Request


```
{
  "name": "MasterNewGroup",
  "displayName": "Master GRP12",
  "description": "",
  "applicationId": "2",
  "parentGroup": "Default",
  "policyName": "Default",
  "_id": "677bdeffa2ed343c1cbedb28",
  "groupBusinessInfo": {
      "firstName": "",
      "lastName": "",
      "contactName": "",
      "phoneNumber": "",
      "lobName": "",
      "costCenter": "",
      "environmentName": "",
      "inventoryNumber": "",
      "email": ""
  },
  "groupLevelCertConfig": {
      "autoPushFlag": false,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "groupOverrideFlag": false,
    "connectorStatusToSkip": [],
    "autoRenewConfig": {
      "renewBefore": 0,
      "autoRenewalFlag": false,
      "approvalRequiredFlag": false
    },
    "autoRegenerateConfig": {
      "regenerateBefore": 0,
      "autoRegenerateFlag": false,
      "approvalRequiredFlag": false
    }
  }
}
```


Sample Response


```
{
  "response": true,
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Delete a Certificate Group

This API is used to delete an existing certificate group.

Before you Begin

- The user should have the required ACF permissions to delete the certificate group.

Request Structure

Endpoint:	/certificate/group
Type:	DELETE
Action:	certificate-group-delete
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?groupName=<groupName>&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
groupName *Header*	(Mandatory) Name of the certificate group to be deleted
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response for the group deletion operation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: Boolean
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	View certificate group action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
417 Expectation failed	CERT-GRP-0002	Default group cannot be deleted.
417 Expectation failed	CERT-GRP-0007	User does not permission to make changes to this group. **Remediation**: Ensure that the requisite RW permissions are assigned to the user for group deletion.
417 Expectation failed	CERT-GRP-0022	Can't delete root level groups with children below it. **Remediation**: Root/parent group with children cannot be deleted.

Sample Request/Response

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group?groupName=MasterGroup1&gwsource=external
```

Sample Response

```
{
  "response": "Certificate Group Deleted successfully",
  "message": "Certificate Group Deleted successfully",
  "appStatusCode": null,
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "tags": {},
  "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Assigning ACL Permissions for Resources

This API manages ACL (Access Control List) permissions for a resource by assigning or revoking access rights for user groups.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you Begin

- The user must have admin privileges or specific ACL management permissions to modify the access control settings.

Request Structure

Endpoint:	resource/certificate/group
Type:	POST
Action:	cert-acl-save-permissions
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/resource/certificate/group?resourceName=<resourceName>&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if **sessionId** is not provided.
Content-Type	(Mandatory) Specifies the nature of the data in the payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Header	**Type**: String **Constraint**: Value of the parameter should be **'application/json'**
resourceName *Header*	(Mandatory) Name of the resource for which the ACL permissions are to be modified **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the POST request. **Type**: Payload

Payload

Payload

Name	Description
assignedObjects	(Optional) Array of user groups and the specific access permissions granted to each **Type**: assignedObjects
unAssignedObjects	(Optional) Array of user groups and the specific access permissions to be revoked from each **Type**: unAssignedObjects

assignedObjects

Name	Description
accessMode	(Mandatory) Level of access to be granted to the group **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

assignedObjects (continued)

Name	Description
	Possible values: **R** (Read-only access), **RW** (Read-Write access)
groupName	(Mandatory) Name of the certificate group being assigned the specified access permissions **Type**: String

unAssignedObjects

Name	Description
accessMode	(Mandatory) Level of access to be revoked from the group **Type**: String **Possible values**: **R** (Read-only access), **RW** (Read-Write access)
groupName	(Mandatory) Name of the certificate group from which the specified access permissions have to be revoked **Type**: String

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response.

response

Name	Description
httpStatusCode	HTTP status code indicating the outcome of the API request.
message	Success message or failure description in case of error.
data	Additional data related to the API response, if applicable
totalCount	Total number of certificate groups affected

Status codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	Deletion action has been triggered successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
404 Not Found	NO_RECORDS_FOUND	No matching records found. **Remediation**: Check and ensure that the values provided for commonName / serialNumber / resourceId are correct.
400 Bad Request	INVALID_REQUEST	Please give valid common name and serial number or resourceId.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Provide a valid commonName and serialNumber or resourceId.
400 Bad Request	INVALID_REQUEST	Please provide a valid action. **Remediation**: Provide a valid action.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - action. **Remediation**: Ensure that the **action** field is available in the request payload.
404 Not Found	CERT-GRP-0003	Groups not found in inventory **Remediation**: Ensure that the group name provided in the request is correct. If the issue still persists, contact AppViewX support.
400 Bad Request	VALIDATION_ERROR_0004	Validation Failure: Field 'accessMode' does not have the expected value **Remediation**: Ensure that **accessMode** has the correct access permission values.

Sample Request/Response

Sample Request

```
{
  "assignedObjects": [
    {
      "accessMode": "RW",
      "groupName": "MasterGroup11"
    },
    {
      "accessMode": "R",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "groupName": "MasterGroup5"
      }
   ],
  "unAssignedObjects": [
     {
        "accessMode": "R",
        "groupName": "Testgroup"
      }


  ]
}
```


Sample Response


```
{
  "response": {
     "httpStatusCode": 200,
     "message": "Successfully assigned / unassigned certificate groups data for null",
     "data": null,
     "totalCount": 0
  },
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **HostName**: A human-readable label assigned to a device (host) on a network

  The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Trigger Profile Sync for Devices

The API initiates the synchronization process for the device profile specified in the payload. Profile synchronization can be triggered for only one device at a time.

Before you begin

- The user should have the ACF permission to view the job scheduler settings.
- The device to be synced should be present in Appviewx and in **Managed** state.
- The user should have **R** or **RW** permission to the device specified.

Request Structure

Endpoint:	/certificate/profiles/sync
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/profiles/sync?gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory only if **sessionID** is not provided) Username for logging in to AppViewX **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password for logging in to AppViewX **Type**: String
Content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
deviceName	(Mandatory) Name of the device for which the profile synchronization must be triggered **Type**: String **Constraint**:
syncType	(Optional) Type of data or configurations to be synchronized for the specified device **Type**: List **Constraint**: Currently, only **profiles** is supported, which ensure that all device profiles, for the specified device, are updated. `syncType = profiles` is also the default value. **Future Support**: Additional sync types may be introduced in the future to support other device-related data and configurations.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the profile sync **Type**: response
message	Success message or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
	Type: String
tags	Additional information in case of failure response

response

Name	Description
deviceName	Name of the device for which the profile sync has been triggered
category	Category of the device for which the profile sync has been triggered
deviceProfiles	List of profiles associated with the specified device **Type**: deviceProfiles
certificateList	List of certificates associated with the specified device
trustedCertificateList	List of trusted certificates associated with the specified device
applicationConnectors	List of application connectors associated with the specified device
deviceWithFailureMessage	Details of sync failures
alerts	List of alerts configured for the device

deviceProfiles

Name	Description
profileId	Unique identifier for the device profile
vendor	Name of the device vendor
deviceName	User friendly name assigned to the device
vendorCategory	Category of the device vendor
profileIdentifierForView	Identifier used for displaying the profile
profileDisplayOrder	Order in which the profile attributes will be displayed
connectorType	Type of the application connector associated with the device profile (profile connector or default connector)
applications	List of applications associated with the device profile

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

deviceProfiles (continued)

Name	Description
hollisticViewData	Holistic list of profile attributes **Type**: holisticViewData
overviewData	Summary of profile details
inventoryData	Inventory-related profile data
vendorProperties	Additional device vendor-specific details **Type**: vendorProperties

hollisticViewData

Name	Description
partition	Device partition assigned to the profile
profileName	Name of the profile
SSL Type	SSL type of the profile

vendorProperties

Name	Description
partition	Name of the partition associated with the device
partitionNameWithoutPath	Name of the partition without path formatting
iAppProfile	Indicates if this profile is an iApp-managed profile

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	null	200 OK Response with the device profiles information
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	AVX-VLDTN-001	Invalid payload data **Remediation**: Ensure that the input values mentioned in the payload are valid.
400 Bad Request	INVALID_REQUEST	Invalid request specified. **Remediation**: Ensure that the payload is valid.
404 Not Found	ERR_DEVICE_UNAVAILABLE	Given device is not available **Remediation**: Ensure that the device specified is available in the inventory.
417 Expectation Failed	ERR_DEVICE_STATUS	Sync is not supported for device with status: Inprogress **Remediation**: Ensure that the device specified is managed.
403 Forbidden	USER_DOES_NOT_HAVE_PERMISSION	The user does not have R or RW permission to the device to perform the sync. **Remediation**: Ensure that the user has the requisite permissions.

Sample Request/Response

Request Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

{ "deviceName": "Certificate_BVT_F5V13_StandAlone",

"syncType": ["PROFILES"] }

Response

{

"response": {

"deviceName": "Certificate_BVT_F5V13_StandAlone",

"category": "ADC",

"deviceProfiles": [

{

"profileId": "Certificate_BVT_F5V13_StandAlone:@Common",

"vendor": "F5",

"deviceName": "Certificate_BVT_F5V13_StandAlone",

"vendorCategory": "ADC",

"profileIdentifierForView": "Certificate_BVT_F5V13_StandAlone:Common",

"profileDisplayOrder": "Partition:@Profile Name:@SSL Type",

"connectorType": "DEFAULT_CONNECTOR",

"applications": [],

"hollisticViewData": {

"Partition": "Common",

"Profile Name": "NA",

"SSL Type": "NA"

},

"overviewData": {},

"inventoryData": {},

"vendorProperties": {

"partition": "Common",

"partitionNameWithoutPath": "Common",

"iAppProfile": false

}

}

],

"certificateList": [],

"trustedCertificateList": [],

"applicationConnectors": [],

"deviceWithFailureMessage": {},

"alerts": []

},

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"message": null,
"appStatusCode": null,
"tags": {},
"headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

List Certificates with Application Connector Details

This API is used to fetch the complete list of certificates in the inventory along with the corresponding application connector details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you Begin

- The user should have the following ACF permissions:

  CERT+ > **Certificate Inventory** > {Certificate_Type}> **View inventory**

  Here, {Certificate_Type}: Server, Client and Code signing

Request Structure

Endpoint:	certificate/list
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/list?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory only if **sessionID** is not provided) Username for logging in to AppViewX **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password for logging in to AppViewX **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
nextPageToken	(Optional; not required for fetching the first set of results) Reference point for fetching the subsequent set of list of certificates, with application connector details, that the user has access to The **certificate/list** API fetches only a limited set of results on each execution. The **nextPageToken** paramter is used as a reference point to continue fetching the next set of results. The **nextPageToken** value returned in the API's response can be used in the next request payload. **Type**: String
searchOptions	(Optional) Additional criteria to filter the search results

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: searchOptions

searchOptions

Name	Description
limit	(Optional) Number of records to be fetched in the response **Type**: Integer **Default value**: 100 **Constraints**: The value should be a valid integer <= 1000. If limit > 1000, the value is capped at 1000.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response

Name	Description
data	Certificate details **Type**: data
nextPageToken	A continuation token for fetching the next batch of certificate details

data

Name	Description
commonName	Certificate common name
serialNumber	Serial number of the certificate
issuerCommonName	Common name of the issuing Certificate Authority
status	Status of the certificate
associatedObjects	Applications, services, or systems where the certificate is being used or linked
discoverySources	Source from where the certificate was certificate
subjectOrganization	Name of the organization that requested the certificate
subjectOrganizationUnit	Name of the business unit within the organization that requested the certificate
subjectLocality	Locality of the organization that requested the certificate
subjectState	State in which the organization that requested the certificate is located
subjectCountry	Country in which the organization that requested the certificate is located
issuerOrganization	Organization name of the issuing Certificate Authority
issuerOrganizationUnit	Buisiness unit name of the issuing Certificate Authority
issuerLocality	Locality of the issuing Certificate Authority

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

data (continued)

Name	Description
issuerState	State in which the issuing Certificate Authority is located
issuerCountry	Country in which the issuing Certificate Authority is located
version	Certificate version
validFrom	Starting date of the certificate's validity period
validTo	Ending date of the certificate's validity period
firstDiscoveryDate	Timestamp the certificate was first discovered
lastBeforeDiscoveryDate	Timestamp of the previous discovery before the most recent one
lastDiscoveryDate	Timestamp of the latest discovery
firstDiscoveryDateStr	Timestamp the certificate was first discovered
lastBeforeDiscoveryDateStr	Timestamp of the previous discovery before the most recent one
validFor	Certificate validity period
keyAlgorithmAndSize	Algorithm and key size used for private key encryption
signatureAlgorithm	Details of the signing algorithm used
signatureHashAlgorithm	Details of the hash algorithm used
keyUsage	Defines permitted uses of the certificate
extendedKeyUsage	Defines additional usage of the certificate
basicConstraints	Defines if the certificate is a CA certificate or an end certificate For a CA certificate, it also specifies how many certificates can be present below in the certficate chain
group	Certificate group mapped to this certificate
subjectAlternativeNames	Subject Alternative Names (SAN) for the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

data (continued)

Name	Description
complianceStatus	Indicates if the certificate complies with the associated policies
applications	List of installed profiles containing the certificate
policyIdentifiers	Unique identifiers of the policies associated with the certificate
expiryStatus	Indicates if the certificate is expired or not
permission	Permissions granted to the certificate
category	Certificate category
uuid	Unique identifier assigned to the certificate
id	Resource ID
certificateAuthority	Issuing certificate authority
authorityKeyIdentifier	Provides the key identifier of the Issuing CA certificate that signed the SSL certificate
subjectKeyIdentifier	Identifier of the certificate itself, specified within the certificate
issuerSerialNumber	Serial number assigned to the issuing Certificate Authority
authorityInfoAccess	Provides information on how to access resources related to the certificate's issuer, such as the issuer's certificate or OCSP responder for revocation checks
certificatePolicies	Certificate policies associated with the certificate
crlDistributionPoints	URL of the Certificate Revocation List
thumbprintAlgorithm	A mathematical process that generates a unique, fixed-size "fingerprint" or digest of a certificate's data, used for verification and identification
thumbPrint	A unique identifier for a certificate, generated by a hash function (like SHA-1 or SHA-256) from the certificate's data, used for verification and identification

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

data (continued)

Name	Description
type	Certificate type
certAttributes	A nested JSON that contains the key-value pairs for the attributes added for the certificate
customAttributes	Attributes with additional certificate metadata details
issuingTemplate	A set of policies and rules that a Certification Authority (CA) uses to guide how it handles certificate requests, including parameters like validity period, encryption, and signature requirements
csrGenerationSource	Source of the certificate CSR generation
certificateHSMDetails	Details of the HSM used for CSR generation
deviceDetails	Details of the device on which the certificate was discovered
csrAvailable	Indicates if valid CSR is available for the certificate
enhancedSANTypes	Subject alternative names (SAN) for the certificate
autoRenewDate	Date of certificate auto renewal
autoRegenDate	Date of certificate auto regeneration
missingParamsForAutoRenew	Missing parameters obstructing certificate auto renewal
caConnectorName	Name of the application connector associated with the certificate
caSettingName	Name of the CASetting created in AppViewX for the chosen certificate authority
suspendedCertificate	Flag indicated if certificate is suspended or not
comments	Additional details related to the certificate
mailAddress	Email address of the organization requesting the certificate
streetAddress	Street address of the organization requesting the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

data (continued)

Name	Description
postalCode	Postal code address of the organization requesting the certificate
publicKeyModulus	Part of the public key used for encryption and signature verification, specifically the modulus value in the RSA algorithm
requestIds	IDs of the workflows associated with the certificate
orderId	Order ID of the certificate
publicKey	Public key associated with the certificate
ellipticCurve	If the keyType chosen is EC, then the ellipticCurve is specified depending on the bit length selected
issuedByRootCertificate	Indicates if certificate was issued directly by a root certificate
cumulativeSanCount	Number of SANs assigned to the certfiicate
caCertificateType	Certificate type used by the Certificate Authority
subject	Certificate subject
discoveryTypes	Discovery scan type used for discovering the certificate
certLifeCycleAction	Last CLM action performed
certLifeCycleActionTimestamp	Timestamp of the last CLM action performed
customExtensions	Any specific OIDs configured for the certficate
deviceNames	Devices for which the certificate has application connectors present
deviceProfiles	Device profiles for which the certificate has application connectors present
certSyncStatus	Provision to manage certificates after discovery
applicationCount	Number of applications associated with the certificate
applicationConnectors	Details of the application connectors associated with the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

data (continued)

Name	Description
applicationConnectorId *applicationConnectors*	Unique identifier assigned to the application connector
vendorConnectorId *applicationConnectors*	Unique identifier assigned to the vendor of the device the certificate is being pushed to
generalInformation *applicationConnectors*	General details related to the application connector
deviceProfile *generalInformation*	Profile details of the device the certificate will be pushed to
vendor *generalInformation*	Name of the vendor of the device the certificate is being pushed to
name *generalInformation*	Name of the application connector
description *generalInformation*	Additional details related to the application connector
certSyncStatus *generalInformation*	Indicates the provision to manage certificates after discovery
category *generalInformation*	Category of the vendor of the device to which the certificate is being pushed
deviceName *generalInformation*	User friendly name assigned to the device to which the certificate is being pushed
certificateDetails	Certificate details associated with the device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

data (continued)

Name	Description
applicationConnectors	
pushDetails *applicationConnectors*	Configuration details related to pushing the certificate
securePush *pushDetails*	Indicates if secure push is enabled This option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.
connectorType *pushDetails*	Indicates if the connector is associated with a profile or is a default connector (not associated with a profile)
pushAutomatically *pushDetails*	Indicates if auto push is enabled for the certificate
overwrite *pushDetails*	Indicates if the overwrite option is enabled for the certificate The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed.
privatekeyAvaliable	Indicates if the certificate private key is available

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	Response with the list of certificates (100 default and upto 1000 based on limit set) and their app connector details

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Invalid **nextPageToken** **Remediation**: Invalid **nextPageToken**. Please ensure the correct **nextPageToken** is sent.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API **Remediation**: • Ensure that the given user has the proper ACF permissions to add comments to the respective certificates. • For the respective role mapped to the user check under - **CERT +>** > {Certificate_Type} > **View Inventory**. {Certificate_Type}: Server, Client and Code signing
403 Forbidden	CERT-ACF-0058	User does not have relevant permission to perform this action. **Remediation**: Ensure the given user has the proper ACF permissions for the respective certificate category (categories: server, client, and code signing).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Request/Response

Request Payload (first request)

```
{
"searchOptions" :{"limit":1000}
}
```

Request Payload (subsequent requests)

```
{
"searchOptions" :{"limit":1000},
"nextPageToken":"67d6ce66f6efc33357f91199"
}
```

Response


```
{
  "response": {
    "data": [
      {
        "commonName": "xzcxzc",
        "serialNumber": "18:F7:58:A2:EE:AB:A3:D8",
        "issuerCommonName": "AppViewX Intermediate CA",
        "status": "Monitored",
        "avxStatus": "Monitored",
        "associatedObjects": [
          "IBM_MQServer:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind"
        ],
        "discoverySources": [
          "IBM_MQServer"
        ],
        "subjectOrganization": "",
        "subjectOrganizationUnit": "",
        "subjectLocality": "",
        "subjectState": "",
        "subjectCountry": "",
        "issuerOrganization": "AppViewX Inc",
        "issuerOrganizationUnit": "",
        "issuerLocality": "Seattle",
        "issuerState": "Washington",
        "issuerCountry": "US",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "version": "3",
        "validFrom": 1586691547000,
        "validTo": 1618227547000,
        "firstDiscoveryDate": 1742227505601,
        "lastBeforeDiscoveryDate": 1742227505601,
        "lastDiscoveryDate": 1742227505601,
        "firstDiscoveryDateStr": null,
        "lastBeforeDiscoveryDateStr": null,
        "validFor": "0 day(s)",
        "keyAlgorithmAndSize": "RSA 4096",
        "signatureAlgorithm": "SHA256withRSA",
        "signatureHashAlgorithm": "SHA256",
        "keyUsage": "DigitalSignature, KeyEncipherment",
        "extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2) ",
        "basicConstraints": "Subject Type=End entity, Path Length=none",
        "group": "Default",
        "subjectAlternativeNames": [
            "DNS : xzcxzc"
        ],
        "complianceStatus": "Compliant",
        "applications": [],
        "policyIdentifiers": [],
        "expiryStatus": "Expired",
        "permission": "RW",
        "category": "Server",
        "uuid": "04b02861eb66fda5a6b423c537b91a9f2c915a95",
        "id": "67d848328419ca79a24779cc",
        "certificateAuthority": "AppViewX",
        "authorityKeyIdentifier": "59:0F:79:63:FA:24:10:3B:65:25:A1:09:94:92:1D:96:6C:3D:DC:EA",
        "subjectKeyIdentifier": "BD:50:5E:52:8E:CE:49:5E:66:ED:99:9C:8D:86:3C:A6:22:44:31:4E",
        "issuerSerialNumber": "A7:F0:67:77:C1:FB:00:0F",
        "authorityInfoAccess": [
            "AuthorityInfoAccess : [ accessMethod : 1.3.6.1.5.5.7.48.1, alterativeName : , url :
http:192.168.133.39/controller/avxocsp?issuerserialnumber=12101285962797744143 ]"
        ],
        "certificatePolicies": [],
        "crlDistributionPoints": [
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "CrlDistributionPoint : [ name : , url : http:192.168.133.39/controller/avxcrl?crlFileName=12101285962797744143.crl ]"
        ],
        "thumbprintAlgorithm": "SHA-1",
        "thumbPrint": "9C:5A:7B:1C:BC:88:86:EE:AD:3D:2C:78:C0:79:1B:CF:4B:23:15:3A",
        "type": "Others",
        "genericFields": null,
        "certAttributes": null,
        "customAttributes": null,
        "validFromDate": null,
        "validToDate": null,
        "discoveredFileNames": [
            "IBM_MQServer::/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb"
        ],
        "issuingTemplate": null,
        "csrGenerationSource": null,
        "certificateHSMDetails": null,
        "deviceDetails": null,
        "newConnectors": [],
        "csrAvailable": false,
        "enhancedSANTypes": null,
        "autoRenewDate": "",
        "autoRegenDate": null,
        "missingParamsForAutoRenew": null,
        "base64ImageContent": null,
        "caConnectorName": null,
        "caSettingName": null,
        "suspendedCertificate": false,
        "comments": null,
        "mailAddress": "",
        "streetAddress": "",
        "postalCode": "",
        "publicKeyModulus": null,
        "requestIds": null,
        "orderId": null,
        "publicKey":
"30:82:02:0A:02:82:02:01:00:AB:F4:AC:96:18:27:78:15:75:4D:20:C5:20:7E:76:72:7D:39:EC:C6:1F:67:6A:03:F6:42:25:A4:A1:5E:99:FF:D8:0B:CC:CD:67:30:57:D
A:95:AA:3C:6C:46:CA:02:FD:8B:26:6C:FC:BC:E7:1A:95:BC:D8:4B:96:4E:D2:ED:0A:C6:BD:3E:72:85:7B:36:F6:9E:78:DA:7C:D9:48:1F:26:72:C6:B1:31:BD:9F:3D
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

:F7:90:AD:63:E1:31:D6:4E:05:A5:2D:F6:C7:3E:84:3E:9A:CF:A2:F5:93:F2:97:66:1E:E9:18:D3:1E:6C:B4:30:12:E5:B0:4B:18:0A:F7:66:35:5C:29:C1:6C:57:DE:86:89:56:C2:37:A1:85:33:14:E0:9C:AD:A0:4A:D1:BE:CB:46:FA:1D:E6:5A:D3:4B:04:2E:14:25:35:50:D3:38:52:90:1D:45:0E:79:B7:D1:72:15:B9:6F:57:AD:87:4C:21:48:F4:51:69:77:CD:A3:C9:B2:5F:FD:FB:EE:9A:22:51:38:C2:2E:1E:7A:7C:82:CF:29:B9:4A:30:66:2E:5F:15:62:39:26:B6:EC:95:C4:04:27:65:5F:90:84:91:78:97:6B:F9:E4:17:F1:2F:2F:91:FE:50:B3:7C:CF:77:4E:69:14:F3:9A:43:F0:D1:9F:6B:02:DE:FF:2E:E0:EB:5D:C6:1C:8F:70:F0:BA:C4:DE:3C:AA:55:87:F3:A6:7B:48:F0:DF:B9:68:4C:01:B6:2D:14:60:CA:D2:09:77:51:BC:D1:5C:F5:E5:01:E5:02:1E:F7:50:20:44:14:1B:C8:B0:F1:02:75:7E:1C:6D:E9:C3:0B:E3:E2:E8:A2:81:1E:67:63:35:B3:DC:BD:CB:61:C9:AA:87:13:1A:49:EA:09:EA:84:C7:BB:B3:17:8F:3C:6E:CB:D1:12:18:00:ED:41:26:12:69:C1:F7:80:0D:6F:6A:2A:C4:EB:7B:85:84:48:A3:BD:6C:8A:9B:D2:E7:70:7E:32:BD:8F:DE:4A:C5:32:A1:0F:51:E2:7D:B2:71:A2:89:6B:A4:2C:79:88:AA:D8:FA:39:EA:67:10:09:89:D3:C1:40:DA:3C:9C:69:AF:E0:9D:2D:C4:7F:CA:3A:CC:48:D4:B0:71:F6:4A:4C:61:ED:14:70:57:0A:20:9F:72:37:5F:3C:9F:84:F1:57:7B:54:99:6E:26:E2:79:55:B4:63:C0:1E:FA:F9:E4:51:58:93:D7:5B:31:BE:13:DD:86:9F:28:58:5A:E5:43:68:DC:7D:02:B3:18:D2:A1:E5:97:6F:6C:D4:36:D6:55:89:38:AF:51:71:BA:96:4A:6B:32:51:42:62:95:02:03:01:00:01",
    "ellipticCurve": null,
    "issuedByRootCertificate": false,
    "cumulativeSanCount": 1,
    "chainPriority": 0,
    "caCertificateType": null,
    "templateProfile": null,
    "certificateTags": null,
    "resourceTags": null,
    "ocspStatus": null,
    "enrollmentMethod": null,
    "kubeService": null,
    "subject": "CN=xzcxzc",
    "discoveryTypes": [
      "Server"
    ],
    "certLifeCycleAction": null,
    "certLifeCycleActionTimestamp": 0,
    "isSsoActive": null,
    "customExtensions": null,
    "deviceNames": [
      "IBMClient_Linux",
      "IBM_MQServer"
    ],
    "deviceProfiles": [
      "IBMClient_Linux:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind",
      "IBM_MQServer:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind"
    ],
    "certSyncStatus": [

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "syncronized",
            "syncronized"
        ],
        "applicationCount": "2",
        "applicationConnectors": [
            {
                "applicationConnectorId":
"IBMClient_Linux:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind:@04b02861eb66fda5a6b423c537b91a9f2c915a95",
                "vendorConnectorId": "67d8482fafab49654c8af0a2",
                "generalInformation": {
                    "deviceProfile": "IBMClient_Linux:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind",
                    "vendor": "IBMClient",
                    "name": "Server IBMClient Connector",
                    "description": "Connector from discovery",
                    "certSyncStatus": "syncronized",
                    "category": "Server",
                    "deviceName": "IBMClient_Linux"
                },
                "certificateDetails": {
                    "rootAndInterCertExist": true,
                    "profileType": "label",
                    "certDirectoryPath": "/var/mqm/qmgrs/TEST1/ssl",
                    "sslCertFilePath": "/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb",
                    "rootCertLabel": "ttr",
                    "serverCertLabel": "ind",
                    "intermediateCertLabel": "ttl",
                    "certificateType": "KDB-.kdb"
                },
                "pushDetails": {
                    "securePush": "false",
                    "connectorType": "Profile Connector",
                    "pushAutomatically": "false",
                    "overwrite": "false"
                },
                "hiddenUiFields": null,
                "validationSettings": {
                    "validationType": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                "customApplications": null,
                "defaultApplications": null
            }
        },
        {
            "applicationConnectorId":
"IBM_MQServer:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind:@04b02861eb66fda5a6b423c537b91a9f2c915a95",
            "vendorConnectorId": "67d848308419ca79a247791b",
            "generalInformation": {
                "deviceProfile": "IBM_MQServer:@KDBLabel:@/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb:@ind",
                "vendor": "MQServer",
                "name": "Server MQServer Connector",
                "description": "Connector from discovery",
                "certSyncStatus": "syncronized",
                "category": "Server",
                "deviceName": "IBM_MQServer"
            },
            "certificateDetails": {
                "rootAndInterCertExist": true,
                "profileType": "label",
                "certDirectoryPath": "/var/mqm/qmgrs/TEST1/ssl",
                "sslCertFilePath": "/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb",
                "rootCertLabel": "ttr",
                "serverCertLabel": "ind",
                "intermediateCertLabel": "ttl",
                "certPathChecksum": "/var/mqm/qmgrs/TEST1/ssl/scb_multichain.kdb$@4290636108",
                "qManagerName": "TEST1",
                "certificateType": "KDB-.kdb"
            },
            "pushDetails": {
                "securePush": "false",
                "connectorType": "Profile Connector",
                "pushAutomatically": "false",
                "overwrite": "false"
            },
            "hiddenUiFields": null,
            "validationSettings": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                    "validationType": null,
                    "customApplications": null,
                    "defaultApplications": null
                }
            }
        ],
        "cvss": 6.8,
        "privatekeyAvaliable": true
    }
  ],
  "nextPageToken": "67d848328419ca79a24779cc"
 },
 "message": null,
 "appStatusCode": null,
 "tags": {},
 "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

List Certificate Groups

This API is used to fetch the list of certificate groups the specified user has access to.

Before you Begin

- The user should have the following ACF permissions:
  - **CERT+** > **Group**
  - **Policy** > **Group** >**View Group**

Request Structure

Endpoint:	certificategroup/list
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificategroup/list?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String **Constraint**: Required if username and password are not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
username *Header*	(Mandatory only if **sessionID** is not provided) Username for logging in to AppViewX **Type**: String
password *Header*	(Mandatory only if **sessionID** is not provided) Password for logging in to AppViewX **Type**: String
content-type *Header*	(Mandatory) Payload content-type with application/json value. **Type**: String **Constraint**: The value must be **application/json**.
gwsource *Query*	(Mandatory) The source from which the request is triggered, e.g., external. **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
nextPageToken	(Optional; not required for fetching the first set of results) Reference point for fetching the subsequent set of certificate groups the user has access to The **certificategroup/list** API fetches only a limited set of results on each execution. The **nextPageToken** paramter

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	is used as a reference point to continue fetching the next set of results. The **nextPageToken** value returned in the API's response can be used in the next request payload. **Type**: String
searchOptions	(Optional) Additional criteria to filter the search results **Type**: searchOptions

searchOptions

Name	Description
limit	(Optional) Number of records to be fetched in the response **Type**: Integer **Default value**: 100 **Constraints**: The value should be a valid integer <= 1000. If limit > 1000, the value is capped at 1000.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success message or failure description in case of error. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Response

Name	Description
data	Details of the certificate groups the user has access to
name *data*	Name of the certificate group
displayName *data*	User friendly name assigned to the certificate group
description *data*	Additional details related to the certificate group
appID *data*	Organization ID associated with the certificate group
policyName *data*	Certificate policy associated with the group
appPolicyName *data*	
permission *data*	Access permissions assigned to the certificate group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
groupBusinessInfo *data*	Details of the business unit associated with the certificate group
contactName *groupBusinessInfo*	Contact of the associated business unit's contact person
firstName *groupBusinessInfo*	First name of the associated business unit's contact person
lastName *groupBusinessInfo*	Last name of the associated business unit's contact person
phoneNumber *groupBusinessInfo*	Phone number of the associated business unit's contact person
lobName *groupBusinessInfo*	Name of the business unit associated with the certificate group
costCenter *groupBusinessInfo*	Code/label of the cost center associated with the certificate group
environmentName *groupBusinessInfo*	Business unit environment associated with the certificate group
inventoryNumber *groupBusinessInfo*	Inventory tracking number for the certificate group
email *groupBusinessInfo*	Email address of the associated business unit's contact person
keywordSet	Keywords associated with the listed certificate group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
data	
groupLevelCertConfig *data*	Configuration details for the certificates that will be associated with the group
autoPushNeededAfterRenewReissue *groupLevelCertConfig*	Indicates if certificates associated with this group will be automatically pushed after they are renewed/reissued
isGroupOverrideEnabled *groupLevelCertConfig*	Indicates if the group level settings for auto renewal/ regeneration will override the certificate level settings
appConnectorSyncStatusListToDelete *groupLevelCertConfig*	List of application connectors to be deleted
autoRenewConfig *groupLevelCertConfig*	Specifies the auto renewal-related configuration details for this certificate group
renewBefore *autoRenewConfig*	For the certificates associated with this group, indicates how many days prior to a certificate's expiry the renewal process will start
autoRenewal *autoRenewConfig*	Indicates if auto renewal is enabled for the certificates associated with this group
manuallyTriggered *autoRenewConfig*	Specifies if the renewal process requires manual triggering
approvalRequiredForAutoRenew *autoRenewConfig*	Indicates if approval is required before certificate renewal is triggered
autoRegenerateConfig *groupLevelCertConfig*	Indicates the auto regeneration-related configuration details for this certificate group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
reportingTo *data*	Indicates the business entity this certificate group reports to
reportingPath *data*	Indicates the group hierarchy structure
updateChild *data*	Indicates if child groups have to be updated
reportedBy *data*	Gives information about who reported this group
deleteRestricted *data*	Indicates if this certificate group can be deleted
_id *data*	Unique identifier assigned to the certificate group
nextPageToken	A continuation token for fetching the next batch of certificate groups

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	null	List of certificate groups fetched successfully
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or a valid

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		sessionId is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Invalid **nextPageToken** **Remediation**: Invalid **nextPageToken**. Please ensure the correct **nextPageToken** is sent.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API **Remediation**: • Ensure that the given user has the proper ACF permissions to add comments to the respective certificates. • For the respective role mapped to the user check under - **CERT+**> > **Groups and Policy** > **Group** > **View Group**.

Sample Request/Response

Request Payload (initial request)

```
{
"searchOptions" :{"limit":1000}
}
```

Request Payload (subsequent requests)

```
{
"searchOptions" :{"limit":1000},
      "nextPageToken":"5422a5c96eeec10c12e3f7be"
}
```

Response

```
{
  "response": {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"data": [
  {
    "name": "Certificate-Gateway",
    "displayName": null,
    "description": "",
    "appId": "",
    "policyName": "Certificate-Gateway",
    "appPolicyName": null,
    "permission": "RW",
    "groupBusinessInfo": {
      "contactName": "",
      "firstName": null,
      "lastName": null,
      "phoneNumber": "",
      "lobName": "",
      "costCenter": "",
      "environmentName": "",
      "inventoryNumber": "",
      "email": ""
    },
    "keywordSet": [
      "Certificate-Gateway"
    ],
    "groupLevelCertConfig": {
      "autoPushNeededAfterRenewReissue": true,
      "isGroupOverrideEnabled": false,
      "appConnectorSyncStatusListToDelete": [],
      "autoRenewConfig": {
        "renewBefore": 20,
        "autoRenewal": true,
        "manuallyTriggered": false,
        "approvalRequiredForAutoRenew": false
      },
      "autoRegenerateConfig": null
    },
    "reportingTo": "Default",
    "reportingPath": "Default:@:Certificate-Gateway",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "updateChild": false,
            "reportedBy": null,
            "deleteRestricted": false,
            "_id": "5bac87e10b3e1937a4bb7abe"
        }
    ],
    "nextPageToken": "5bac87e10b3e1937a4bb7abe"
  },
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Use Insights to Create a Centralized CERT+ Dashboard

This API is used to fetch data from the existing Insights reports and visualize it on a CERT+ centralized dashboard. This will allow tenants to view all the data for an individual tenant in a single pane.

With this API, data from the following widgets/reports can be consumed for the visualization on the centralized dashboard:

- CERT+ → Insights → Summary → CryptoScore widget (Including the score and horizontal bars with severity)
- CERT+ → Insights → Google 90-day → Google 90 Day Score (Including the score and horizontal bars with severity)
- CERT+ → Insights → Google 90-day → Non-Standard Certificates (Only numbers for each block, not drill down)
- CERT+ → Insights → Risk & Crypto → Non-Standard Certificates (Only numbers for each block, not drill down)
- CERT+ → Insights → Operation → CLM action trend (Data for Daily, Weekly, Monthly, Quarterly, Yearly)

Before you Begin

- Ensure that the user has the required permissions to access the Insights reports.
- Ensure that the user has the required permissions to execute this API.

Request Structure

Endpoint:	/insights-report
Type:	GET
Action:	insights-report
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/insights-report?reportName=<REPORT_NAME>&groupName=<GROUP_NAME>&periodicity=<Periodocity>&isSync=true&gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type: application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (for example, external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the PUT request. **Type**: Payload

Payload

Payload

Name	Description
reportName	(Mandatory) Report types that have to be fetched for the centralized dashboard **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values (one from the following): • CryptoScore:summary • Google90DayScore:summary • Google90DayScore:non-standard-certificate-count • OperationReport:clm-action-trend • CryptoRiskReport:non-standard-certificate-count
groupName	(Optional) Name of the certificate group for filtering the report data to be fetched **Type**: String **Deafult value**: All certificate groups mapped to the logged in user
periodicity	(Mandatory only for the **OperationReport:clm-action-trend** report type) Time interval for filtering the report data to be fetched **Type**: String **Possible values**(one of the following): • yearly • quarterly • monthly • weekly • daily

Response Structure for the Crypto Score Summary Report

Response Parameters

Name	Description
reports	Object containing report details **Type**: reports
message	Success or failure description **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

reports

Name	Description
name	Report name as specified in the payload
score	A numerical representation that indicates the overall compliance status or risk level
metrics	An object containing a detailed breakdown of the individual parameters for each severity level that contributes to the overall score **Type**: metrics
lastExecutedTime	Timestamp of when the report was last generated

metrics

Name	Description
severity	Risk level category assigned to classify the impact of the issues detected
count	Total no. of certificates that fall under the specified severity level
label	Display label assigned to the severity level
percent	Percentage of certificates that fall under the specified severity level

Response Structure for the Google 90 Day Score Summary Report

Response Parameters

Name	Description
reports	Object containing the report details

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
	Type: reports
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

reports

Name	Description
name	Report name as specified in the payload
score	A numerical representation that indicates the overall compliance status or risk level
metrics	An object containing a detailed breakdown of the individual parameters for each severity level that contributes to the overall score **Type**: metrics
category	A qualitative label to represent the overall score range of the report

metrics

Name	Description
summary	An object containing the detailed breakdown of the individual parameters for each severity level that contributes to the overall score **Type**: summary
total	Total number of certificates evaluated in the report, across severity levels

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

metrics (continued)

Name	Description
non-standard	Number of certificates that are non-compliant to the cryptographic and policy guidelines

summary

Name	Description
severity	Risk level category assigned to classify the impact of the issues detected
count	Total no. of certificates that fall under the specified severity level
label	Display label assigned to the severity level
percent	Percentage of certificates that fall under the specified severity level

Response Structure for the Google 90 Day Non Standard Certificate Count Report

Response Parameters

Name	Description
reports	Object containing the report details **Type**: reports
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

reports

Name	Description
name	Report name as specified in the payload
count	Total number of non standard certificates evaluated in the report

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

reports (continued)

Name	Description
executionTime	Timestamp of when the report was last generated
chartData	An object containing categorized counts of non-standard certificates, grouped by compliance issues **Type**: chartData

chartData

Name	Description
unknownCA	Total number of certificates issued by CAs that are not recognized or trusted
rootCAIssued	Total number of certificates issued by a root CA
sanMismatch	Total number of certificates with Subject Alternative Name (SAN) entries that do not match the domain or resource they're deployed on
unAssociated	Total number of certificates that are not associated with an endpoint
selfSigned	Total number of certificates that are signed by the issuing CA
wildcard	Total number of certificates that use wildcard domains

Response Structure for the Risk & Crypto Non Standard Certificate Count Report

Response Parameters

Name	Description
reports	Object containing the report details **Type**: reports
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
tags	Additional information for the failure response

reports

Name	Description
name	Report name as specified in the payload
count	Total number of non standard certificates evaluated in the report
executionTime	Timestamp of when the report was last generated
chartData	An object containing categorized counts of non-standard certificates, grouped by compliance issues **Type**: chartData

chartData

Name	Description
unknownCA	Total number of certificates issued by CAs that are not recognized or trusted
rootCAIssued	Total number of certificates issued by a root CA
sanMismatch	Total number of certificates with Subject Alternative Name (SAN) entries that do not match the domain or resource they're deployed on
unAssociated	Total number of certificates that are not associated with an endpoint
selfSigned	Total number of certificates that are signed by the issuing CA
wildcard	Total number of certificates that use wildcard domains

Response Structure for the Operation CLM Action Trend Report

Response Parameters

Name	Description
reports	Object containing the report details **Type**: reports

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

reports

Name	Description
name	Report name as specified in the payload
periodicity	Time interval used for filtering the data evaluated by the report
dataList	Object containing timestamped data points and the corresponding count of certificates on which the specified CLM action was performed, collected over the defined periodicity **Type**: dataList

dataList

Name	Description
values	Object containing timestamped data points and certificate index number **Type**: values
action	CLM action used for grouping the data points over the given periodicity

values

Name	Description
x	Timestamp of the action performed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

values (continued)

Name	Description
y	Number of certificates on which the CLM action was executed at the specified timestamp

Status Codes

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason: Invalid credentials **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Mandatory field missing or invalid value **Remediation**: Ensure that the missing mandatory field, as specified in the error response, is included in the payload and is assigned a valid value.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure that the user has all the requisite ACF permissions to assign certificates to the group.
403 Forbidden	CERT-REPORT_1015	User does not have access to the certificate group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that • the certificate group exists in the database • the user has access to the certificate group
417 Expectation Failed	CERT-FV-001	Invalid query parameter **Remediation**: Ensure that the query does not contain an invalid parameter or an invalid value assigned to a valid parameter.
417 Expectation Failed	CERT-FV-001	Null/empty value assigned to a query paramter **Remediation**: Ensure that no query parameters are assigned null/empty values.
417 Expectation Failed	CERT-FV-001	The periodicity parameter is included in the query for a non-compatible report type. **Remediation**: The periodicity parameter is applicable only for the OperationReport:clm-action-trend report.

Sample Request/Response for the Crypto Score Summary Report

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/insights-report?reportName=CryptoScore:summary&groupName=Default&gwsource=external
```

Sample Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
  "response": {
    "score": "10.0",
    "metrics": [
      {
        "severity": "Critical",
        "count": 0,
        "label": "Critical",
        "percent": 0.0
      },
      {
        "severity": "High",
        "count": 0,
        "label": "High",
        "percent": 0.0
      },
      {
        "severity": "Medium",
        "count": 0,
        "label": "Medium",
        "percent": 0.0
      },
      {
        "severity": "Low",
        "count": 0,
        "label": "Low",
        "percent": 0.0
      },
      {
        "severity": "Good",
        "count": 18,
        "label": "Good",
        "percent": 100.0
      }
    ]
  },
  "message": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "appStatusCode": null,
    "tags": {
        "lastExecutedTime": 1751271654306
    },
    "headers": null
}
```


Sample Request/Response for the Google 90 Day Score Summary Report

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/insights-report?reportName=Google90DayScore:summary&groupName=Default&gwsource=external
```

Sample Response


```
{
    "response": {
        "score": "8.8",
        "metrics": {
            "summary": [
                {
                    "severity": "Critical",
                    "count": 0,
                    "label": "2 years or above",
                    "percent": 0.0
                },
                {
                    "severity": "High",
                    "count": 0,
                    "label": "398 days - 2 years",
                    "percent": 0.0
                },
                {
                    "severity": "Medium",
                    "count": 17,
                    "label": "91 - 397 days",
                    "percent": 100.0
                },
                {
                    "severity": "Low",
                    "count": 0,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                "label": "1 - 30 days",
                "percent": 0.0
            },
            {
                "severity": "Good",
                "count": 0,
                "label": "31 - 90 days",
                "percent": 0.0
            }
        ],
        "total": 17,
        "non-standard": 17
    },
    "category": "Excellent"
  },
  "message": null,
  "appStatusCode": null,
  "tags": {
    "lastExecutedTime": 1751271575587
  },
  "headers": null
}
```


Sample Request/Response for the Google 90 Day Non Standard Certificate Count Summary Report

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/insights-report?reportName=Google90DayScore:non-standard-certificate-count&groupName=Default&gwsource=external
```

Sample Response


```
{
  "response": {
    "name": "non-standard-certificate-count",
    "category": "all",
    "executionTime": 1751271208521,
    "chartData": {
      "unknownCA": 0,
      "rootCAIssued": 0,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "sanMismatch": 17,
            "unAssociated": 17,
            "selfSigned": 0,
            "wildcard": 0
        },
        "status": "Completed",
        "delta": false,
        "_id": "non-standard-certificate-count-all"
    },
    "message": null,
    "appStatusCode": null,
    "tags": {
        "lastExecutedTime": 1751271208521
    },
    "headers": null
}
```


Sample Request/Response for the Risk & Crypto Non Standard Certificate Count Summary Report

Sample Request

```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/insights-report?reportName=CryptoRiskReport:non-standard-certificate-count&groupName=Default&gwsource=external
```

Sample Response


```
{
    "response": {
        "name": "non-standard-certificate-count",
        "category": null,
        "executionTime": 1751271424910,
        "chartData": {
            "unknownCA": 0,
            "rootCAIssued": 0,
            "sanMismatch": 17,
            "unAssociated": 18,
            "selfSigned": 0,
            "wildcard": 0
        },
        "status": "Completed",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "delta": false,
        "_id": "non-standard-certificate-count"
    },
    "message": null,
    "appStatusCode": null,
    "tags": {
        "lastExecutedTime": 1751271424910
    },
    "headers": null
}
```


Sample Request/Response for the Operation CLM Action Trend Report

Sample Request


```
https://<IP/HostName/TenantName>:<GWPORT>/avxapi/insights-report?reportName=OperationReport:clm-action-trend&groupName=Default&gwsource=external
```


Sample Response


```
{
    "response": {
        "dataList": [
            {
                "values": [
                    {
                        "x": 1751155200000,
                        "y": 0
                    },
                    {
                        "x": 1751068800000,
                        "y": 0
                    },
                    {
                        "x": 1750982400000,
                        "y": 0
                    },
                    {
                        "x": 1750896000000,
                        "y": 0
                    },
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            {
                "x": 1750809600000,
                "y": 0
            },
            {
                "x": 1750723200000,
                "y": 0
            },
            {
                "x": 1750636800000,
                "y": 0
            }
        ],
        "key": "Revoked"
    },
    {
        "values": [
            {
                "x": 1751155200000,
                "y": 0
            },
            {
                "x": 1751068800000,
                "y": 0
            },
            {
                "x": 1750982400000,
                "y": 0
            },
            {
                "x": 1750896000000,
                "y": 0
            },
            {
                "x": 1750809600000,
                "y": 0
            },
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            {
                "x": 1750723200000,
                "y": 0
            },
            {
                "x": 1750636800000,
                "y": 0
            }
        ],
        "key": "Renewed"
    },
    {
        "values": [
            {
                "x": 1751155200000,
                "y": 0
            },
            {
                "x": 1751068800000,
                "y": 0
            },
            {
                "x": 1750982400000,
                "y": 0
            },
            {
                "x": 1750896000000,
                "y": 0
            },
            {
                "x": 1750809600000,
                "y": 2
            },
            {
                "x": 1750723200000,
                "y": 0
            },
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            {
                "x": 1750636800000,
                "y": 0
            }
        ],
        "key": "Enrolled"
    },
    {
        "values": [
            {
                "x": 1751155200000,
                "y": 0
            },
            {
                "x": 1751068800000,
                "y": 0
            },
            {
                "x": 1750982400000,
                "y": 0
            },
            {
                "x": 1750896000000,
                "y": 0
            },
            {
                "x": 1750809600000,
                "y": 1
            },
            {
                "x": 1750723200000,
                "y": 0
            },
            {
                "x": 1750636800000,
                "y": 0
            }
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            ],
            "key": "Regenerated"
          }
        ]
    },
    "message": "cert clm action trend retrieved successfully",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Assign Certificates to a Group

This API is used to assign one or multiple certificates to an existing certificate group.

Certificate groups simplify certificate lifecycle management, access control, and policy enforcement for certificates.

Before you Begin

- Ensure that the user has the required permissions for the group to which the certificate currently belongs.
- Ensure that the target certificate group exists.
- Ensure that the user has the required permissions to assign certificates to the target certificate group (to which the certificates will be assigned).

Request Structure

Endpoint:	/certificate/group/assign
Type:	PUT
Action:	certificate-group-assign
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group/assign?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (for example, external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the PUT request. **Type**: Payload

Payload

Payload

Name	Description
groupName	(Mandatory) Name of the certificate group to which the certificates have to be assigned **Type**: String
resourceIds	(Mandatory) Comma-separated list of the resource IDs of all certificates that have to be assigned to the above-mentioned certificate group The resources IDs can be retrieved using the /certificate/search API. **Type**: List **Constraints**: Ensure that all certificates belong to the same certificate category.
comment	(Optional) Additional details related to the certificate assignment

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Constraints**: • Maximum character limit is 255. • Special characters and HTML tags are invalid values.

Response Structure

Success Response

200 OK Response with the message: Group assign action successfully performed.

Response content-type: application/json

Response Parameters

Name	Description
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

Status Codes

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason: Invalid credentials **Remediation**: Ensure that valid username and password or a valid

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		sessionId is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Mandatory field missing or invalid value **Remediation**: Ensure that the missing mandatory field, as specified in the error response, is included in the payload and is assigned a valid value.
400 Bad Request	VALIDATION_ERROR_0004	`comment` exceeds the 255-character limit. **Remediation**: Ensure that the text entered as comments in the payload is less than or equal to 255 characters.
400 Bad Request	CERT-GEN-0033	Invalid characters in the comments. **Remediation**: Ensure that the text entered as comments in the payload does not have any special characters or HTML tags.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure that the user has all the requisite ACF permissions to assign certificates to the group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		To enable this, go to (**Menu**) > **CERT+** > **Groups & Policies** > **Group** > **Assign Group**.
403 Forbidden	CERT-ACL-0006	Access denied since user does not have all the requisite permissions to update certificates. **Remediation**: Ensure that the user has all the required ACL resource permissions for assigning the certificates.
403 Forbidden	CERT-ACF-0058	User does not have the relevant permissions to perform this action. **Remediation**: Ensure that the user has the required permissions for updating the required certificate category.
403 Forbidden	CERTIFICATE_BELONG_GROUP_PERMISSION_DENIED	User does not have RW permission for the certificate group to which the certificate already belongs. **Remediation**: Ensure that the user has RW permission for the certificate groups to which all certificates, the resource IDs of which have been listed in the payload, currently belong.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
403 Forbidden	ACF_NOT_AVAILABLE_FOR_SERVER_CERT	User does not have view permission for the server certificate inventory. **Remediation**: Ensure that the user has all the required ACF permissions for viewing the server certificate inventory.
403 Forbidden	ACF_NOT_AVAILABLE_FOR_CLIENT_CERT	User does not have view permission for the client certificate inventory. **Remediation**: Ensure that the user has all the required ACF permissions for viewing the client certificate inventory.
403 Forbidden	ACF_NOT_AVAILABLE_FOR_CODE_SIGNING_CERT	User does not have view permission for the code signing certificate inventory. **Remediation**: Ensure that the user has all the required ACF permissions for viewing the code signing certificate inventory.
404 Not Found	GROUP_NOT_FOUND_OR_PERMISSION_DENIED	The certificate group name mentioned in the payload does not exist or the user does not have RW permission to the group. **Remediation**: Ensure that the certificate group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		mentioned in the payload exists and the user has the required permissions for assigning certificates to the group.

Sample Request/Response

Sample Request


```
{
 "groupName": "Certificate-Gateway",
 "resourceIds": [
  "67bc2ca76a105e1a05691c1c",
  "67bc2ca76a105e1a05691c2c",
  "67bc2ca76a105e1a05691c3c"
 ],
 "comment": "Sample Comment"
}
```


Sample Response


```
{
 "Response":
 {
  "Successful Ids": [
   "67bc2ca76a105e1a05691c1c",
   "67bc2ca76a105e1a05691c2c",
   "67bc2ca76a105e1a05691c3c"
  ],
 },
 "message": "Group assign action successfully performed",
 "appStatusCode": null,
 "Tags": { },
 "Headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Unassign Certificates from a Group

This API is used to unassign one or multiple certificates from an existing certificate group. The unassigned certificates are then assigned to the default certificate group.

Before you Begin

- Ensure the user has the required permissions for accessing the default certificate group.
- Ensure that the user has the required permissions for the group to which the certificate currently belongs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Ensure that the certificate/certificates is/are already assigned to the certificate group.
- Ensure that the user has the required ACF permissions to unassign certificates from the certificate group.

Request Structure

Endpoint:	/certificate/group/unassign
Type:	PUT
Action:	certificate-group-unassign
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/group/unassign?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource	(Mandatory) Source from which the request is triggered. (for example, external)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the PUT request. **Type**: Payload

Payload

Payload

Name	Description
resourceIds	(Mandatory) Comma-separated list of the resource IDs of all certificates that have to be unassigned The resources IDs can be retrieved using the /certificate/search API. **Type**: List
comment	(Optional) Additional details related to the certificate assignment **Type**: String **Constraints**: • Maximum character limit is 255. • Special characters and HTML tags are invalid values.

Response Structure

Success Response

200 OK Response with the message: Group unassign action successfully performed.

Response content-type: application/json

Response Parameters

Name	Description
message	Success or failure description

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String
tags	Additional information for the failure response

Status Codes

HTTP Code	appStatusCode	Response Message
401 Unauthorized	AVX_GW_003	Authentication failed, reason: Invalid credentials **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	VALIDATION_ERROR_0004	Mandatory field missing or invalid value **Remediation**: Ensure that the missing mandatory field, as specified in the error response, is included in the payload and is assigned a valid value.
400 Bad Request	VALIDATION_ERROR_0004	`comment` exceeds the 255-character limit.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the text entered as comments in the payload is less than or equal to 255 characters.
400 Bad Request	CERT-GEN-0033	Invalid characters in the comments. **Remediation**: Ensure that the text entered as comments in the payload does not have any special characters or HTML tags.
403 Forbidden	AVX_GW_005	User does not have access to the targeted API. **Remediation**: Ensure that the user has all the requisite ACF permissions to unassign certificates from the group. To enable this, go to (**Menu**) > **CERT+** > **Groups & Policies** > **Group** > **Assign Group**.
403 Forbidden	CERT-ACL-0006	Access denied since user does not have all the requisite permissions to update certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the user has all the required ACL resource permissions for adding comments to the certificates.
403 Forbidden	CERT-ACF-0058	User does not have the relevant permissions to perform this action. **Remediation**: Ensure that the user has the required permissions for the required certificate category.
403 Forbidden	CERTIFICATE_BELONG_GROUP_PERMISSION_DENIED	User does not have RW permission for the certificate group to which the certificate belongs. **Remediation**: Ensure that the user has RW permission for the certificate groups to which all certificates, the resource IDs of which have been listed in the payload, currently belong.
403 Forbidden	ACF_NOT_AVAILABLE_FOR_SERVER_CERT	User does not have view permission for the server certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the user has all the required ACF permissions for viewing the server certificate inventory.
403 Forbidden	ACF_NOT_AVAILABLE_FOR_CLIENT_CERT	User does not have view permission for the client certificate inventory. **Remediation**: Ensure that the user has all the required ACF permissions for viewing the client certificate inventory.
403 Forbidden	ACF_NOT_AVAILABLE_FOR_CODE_SIGNING_CERT	User does not have view permission for the code signing certificate inventory. **Remediation**: Ensure that the user has all the required ACF permissions for viewing the code signing certificate inventory.
404 Not Found	DEFAULT_CERT_GROUP_PERMISSION_DENIED	User should have RW permissions for the default certificate group before unassigning certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that the user has access to the default certificate group.

Sample Request/Response

Sample Request


```
{
 "resourceIds": [
  "67bc2ca76a105e1a05691c1c",
  "67bc2ca76a105e1a05691c2c",
  "67bc2ca76a105e1a05691c3c"
 ],
 "comment": "Sample Comment"
}
```


Sample Response


```
{
 "Response":
 {
  "Successful Ids": [
   "67bc2ca76a105e1a05691c1c",
   "67bc2ca76a105e1a05691c2c",
   "67bc2ca76a105e1a05691c3c"
  ],
 },
 "message": "Group unassign action successfully performed",
 "appStatusCode": null,
 "Tags": { },
 "Headers": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Archive Certificates

This API is used to archive one or more certificates from the AppViewX inventory, based on the provided request.

Before you Begin

- Ensure that the user has the required permissions for accessing the group to which the certificate currently belongs.
- Ensure that the user has the required ACF permissions for archiving certificates for individual certificate categories (server, client, and code signing).

Request Structure

Endpoint:	/certificate/archive

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/archive?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered (for example, external) **Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the certificate archival request **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
certIds	(Mandatory) List of the UUIDs of the certificates that have to be archived **Type**: List
module	(Mandatory) Certificate category for which archival is enabled on execution of this API **Type**: String **Possible values**: • CERT_SERVER_INV • CERT_CLIENT_INV • CERT_CODE_SIGNING_INV **Constraint**: Only one value (certificate category) can be assigned at a time
archiveReason	(Mandatory) Reason for archiving the specified certificate(s) **Type**: String
archiveComments	(Optional) Additional details related to the certificate archival request **Type**: String

Response Structure

Response Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success or failure description **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String **Possible values**: Status codes
tags	Additional information for the failure response

response

Name	Description
code	Success/failure response code **Type**: String
message	Success or failure message **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Operation completed successfully.
401 Unauthorized	AVX_GW_003	Authentication failed **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	CERT-INV-001	Missing or invalid field(s) in the payload **Remediation**: Ensure that the missing mandatory field, as specified in the error response, is included in the payload and is assigned a valid value.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
404 Not Found	CERT-INV-0021	Certificate not found or user lacks permission. **Remediation**: Ensure that: • the certificate specified for archival is a valid certificate that exists in the inventory • the user requesting the archival has the requisite permissions to do so

Sample Request


```
{
  "certIds": ["4e2d93f07b8d568392ff96bf8e25391f6478f8cd"],
  "module": "CERT_SERVER_INV",
  "archiveReason": "Renewed",
  "archiveComments": "Renewed Cert"
}
```


Sample Response

Sample Response - Success


```
{
  "response": {
    "code": "CERTIFICATE_ARCHIVAL_SUCCESSFULL",
    "message": "Selected certificate(s) has been archived successfully from AppViewX inventory."
  },
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


Sample Response - Failure (Duplicate or permission issue)


```
{
  "response": null,
  "message": "Certificate is not available in the inventory or User doesn't have permission to the Certificate.",
  "appStatusCode": "CERT-INV-0021",
  "tags": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "upstream_error": "true"
  },
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Recover Archived Certificates

This API is used to recover archived certificate(s) and restore them to the active inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you Begin

- Ensure that the user has the required ACF permissions to recover archived certificates.
- Ensure that the user has the required permissions for accessing the group to which the certificate will be moved after recovery.

Request Structure

Endpoint:	/certificate/restore
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/restore?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory if **username** and **password** are not provided) Session ID received after login **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username **Type**: String
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password **Type**: String
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource	(Mandatory) Source from which the request is triggered. (for example, external)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
Payload *Body*	Contains all the parameters to be included in the request body for the certificate recovery request. **Type**: Payload

Payload

Payload

Name	Description
certIds	(Mandatory) List of the UUIDs of the archived certificates that have to be restored **Type**: List
restoreReason	(Mandatory) Reason for restoring the specified certificate(s) **Type**: String

Response Structure

Response Parameters

Name	Description
response	Contains the response attributes **Type**: response
message	Success or failure description **Type**: String
appStatusCode	Application specific status code for the response It is a non-null value for a failure response. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
	Possible values: Status codes
tags	Additional information for the failure response

response

Name	Description
code	Success/failure response code **Type**: String
message	Success or failure message **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Operation completed successfully.
401 Unauthorized	AVX_GW_003	Authentication failed **Remediation**: Ensure that valid username and password or a valid sessionId is provided as header parameters.
400 Bad Request	CERT-INV-001	Missing or invalid field(s) in the payload **Remediation**: Ensure that the missing mandatory field, as specified in the error response, is included in the payload and is assigned a valid value.
404 Not Found	CERT-INV-0021	Certificate not found or user lacks permission.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that: • the certificate specified for restore is a valid certificate that exists in the archived certificates inventory • the user requesting the certificate restore has the requisite permissions to do so

Sample Request

```
{
  "certIds": ["4e2d93f07b8d568392ff96bf8e25391f6478f8cd"],
  "restoreReason": "License Restored"
}
```

Sample Response

Sample Response - Success

```
{
  "response": {
    "code": "CERTIFICATE_RESTORE_SUCCESSFULL",
    "message": "Certificate successfully recovered."
  },
  "message": null,
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```

Sample Response - Failure (Duplicate or permission issue)

```
{
  "response": null,
  "message": "Certificate is not available in the inventory or User doesn't have permission to the Certificate.",
  "appStatusCode": "CERT-INV-0021",
  "tags": {
    "upstream_error": "true"
  },
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

ADC+ API (for CERT+)

- Push and Bind Certificate to ADC Devices
- Push and Bind Certificate to ADC Profile
- Rollback Certificate to ADC profile

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Push and Bind Certificate to ADC Devices

This API initiates a push of the certificate to ADC devices [F5, Citrix, AVI, A10, AmazonELB, NginxPlus, HAProxy] and bind it to a profile or virtual server depending on the ADC device.

Before you begin

Ensure the following before attempting to push a certificate to a particular ADC device through AppViewX:

- ADC devices must be configured in AppViewX.
- The device should be in the Managed state.
- A valid certificate should be used to push the certificate.
- Profiles or virtual servers should be available. This can be fetched using **Fetch Available Profiles API** (refer section below).

Fetch available profiles API

Endpoint:	/certificate/profiles
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/profiles?category=ADC&vendor=F5&deviceName=F5_device&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Details - Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Details - Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
category *Query*	(Mandatory) Specifies the device category. **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor *Query*	(Mandatory) Vendor for the chosen device. For example, **F5** is a vendor for the ADC category. **Type**: String **Possible values**: F5, Citrix, AVI, A10, AmazonELB, NginxPlus, and HAProxy.
certificateUuid *Query*	(Mandatory) Resource id of the certificate. **Type**: String **Constraints**: This can be obtained from search API.
deviceName *Query*	(Mandatory) Name of the device as per AppViewX Device Inventory. **Type**: String
inventory	(Mandatory) Name of AppViewX inventory where the certificate is present.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Details - Parameters (continued)

Name	Description
Query	**Type**: String **Possible values**: Server, Client, Code Signing, and Device.

Response Parameters

Name	Description
response	Contains the following response attributes for the fetch profiles request: objects, totalRecords, obtainedRecords, and obtainedRecordRange. **Type**: List of Objects
objects	List of available device profile Ids. response **Type**: List of String
totalRecords	Total number of profiles fetched. response **Type**: Integer
obtainedRecords	Total number of profiles fetched. response **Type**: Integer
obtainedRecordRange	Range of record found. response **Type**: Object
message	Success message of the action or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description


```
{
 "response": {
 "objects": [
 "device_name",
 "device_name:@apm-default-serverssl:@Common",
 "device_name:@clientssl-insecure-compatible:@Common",
 "device_name:@clientssl-secure:@Common",
 "device_name:@clientssl:@Common",
 "device_name:@crypto-client-default-serverssl:@Common",
 "device_name:@crypto-server-default-clientssl:@Common",
 "device_name:@pcoip-default-serverssl:@Common",
 "device_name:@serverssl-insecure-compatible:@Common",
 "device_name:@serverssl:@Common",
 "device_name:@splitsession-default-clientssl:@Common",
 "device_name:@splitsession-default-serverssl:@Common",
 "device_name:@wom-default-clientssl:@Common",
 "device_name:@wom-default-serverssl:@Common"
 ],
 "totalRecords": 14,
 "obtainedRecords": 14,
 "obtainedRecordRange": {
 "start": 0,
 "end": 0
 }
 },
 "message": "14 record(s) found",
 "appStatusCode": null,
 "tags": {},
 "headers": null
 }
```


Request Structure for Push and Bind SYNC API

Endpoint:	/certificate/profiles/push

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Type:	POST
Sample URL:	*https://<appviewx node id>:<gateway port>/avxapi/certificate/profiles/push?gwkey=f000ca01&gwsource=external&ttl=120*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
ttl *Query*	(Mandatry) The time to live (**ttl**) is a query parameter. If the total time taken surpasses this value, the response will indicate that the request is still in progress. On the other hand, if the operation completes successfully within the TTL, the response will indicate success. **Type**: Integer
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String **Constraint**: Optional if the Uuid of the certificate is present.
certificateUuid	(Optional) Certificate UUid **Type**: String **Constraint**: Mandatory only if certificateId is not present.
selectedProfiles	(Mandatory) ADC device profile id. **Type**: List of String **Constraint**: These can be obtained from Fetch Available Profiles API. • If a Profile connector is specified, then the certificate will be pushed and bound to the profile. • If a Default connector specified, then the certificate will be only pushed.
certificateDetails	(Mandatory) Certificate details for the server devices to be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Any of the following server devices: • Certificate details for F5 • Certificate details for Citrix • Certificate details for AVI • Certificate details for A10 • Certificate details for AmazonELB • Certificate details for NignixPlus • Certificate details for HAProxy

Certificate details for F5

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.crt
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into an F5 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the CA file name and intermediate certificate file name.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into an F5 device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
rootCertificateFileName	(Optional) A user defined file name for pushing the intermediate and root certificates into in a F5 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles": [
 "device_name:@default:@clientssl"
 ],
 "certificateDetails": {
 "certificateFileName": "test123.crt",
 "certificateType": "PEM-.crt",
 "privateKeyFileName": "test123.key",
 "pushRootAndIntermediateCertificates": true,
 "rootCertificateFileName": "test123_root.crt"
 }
 }
```

Certificate details for Citrix

Name	Description
certificateType	(Mandatory) Type of the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
	Type: String **Possible Certificate types**: PEM-.crt, PEM-.cer, PEM-.pem, DER-.der, and DER-.cer
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the Citrix device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the Citrix device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Citrix device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
sniCert	(Optional) Enables the SNI push for certificate. **Type**: Boolean
sniStatus	(Optional) Enables SNI in the virtual server. **Type**: Boolean

Request Payload


```
{
"certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles": [
"device_name:@default:@sslvs"
],
"certificateDetails": {
"certificateFileName": "test123.crt",
"certificateKeyPairName": "test123",
"certificateType": "PEM-.crt",
"intermediateCertificateFileName": [
"test123_inter.crt"
],
"privateKeyFileName": "test123.key",
"pushRootAndIntermediateCertificates": true,
"rootCertificateFileName": "test123_root.crt",
"sniCert": "false",
"sniStatus": "false"
}
}
```


Certificate details for AVI

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
	Possible Certificate types: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the AVI device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the AVI device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
	characters except -, _, .. It should not be the same as the certificate file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PEM-.pem”,
 "certificateFileName":"certificate_push.pem",
 "privateKeyFileName":"certificate_push.key",
 "pushRootAndIntermediateCertificates": true,
 “intermediateCertificateFileNames”:[”test_cert_inter.crt”],
 "rootCertificateFileName": "test_cert_ca.crt"
 }
 }
```

Certificate details for A10

Name	Mandatory
certificateType	(Mandatory) Type of the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
	Type: String **Possible Certificate types**: PEM-.pem, PEM-.crt, PEM-.cer, DER-.der, DER-.cer, PKCS#7-.p7b, PKCS#7-.p7c, PKCS#7-.p12, and PKCS#7-.pfx
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the A10 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the A10 device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pfxPassword	(Optional) Password for the **pfx** and **pkcs12** file type. It is **mandatory** only if the certificate file type is **.pfx** or **.pkcs12**. **Type**: Boolean **Constraints**: The password should be Base64 encoded.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the A10 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request payload for non pfx and p12 cert types

```
{ "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
        "selectedProfiles":[ "device_name:@serverssl-insecure-compatible:@Common" ],
        "certificateDetails":{ “certificateType”:”PEM-.crt”,
        "certificateFileName":"certificate_push.crt",
        "privateKeyFileName":"certificate_push.key", "pushRootAndIntermediateCertificates":
        true, "intermediateCertificateFileNames":[ "test_cert_ca.crt"] } }
```

Request payload for pfx and p12 cert types

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PKCS-.pfx”,
 "certificateFileName":"certificate_push.pfx",
 "pushRootAndIntermediateCertificates": true,
 "intermediateCertificateFileNames":[ “test_cert_ca.crt"],
 “pfxPassword”:”cGFzc3dvcmQ=”
 }
 }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateLocation	(Mandatory) Location of the certificate. Values are **ACM** or **IAM**. **Type**: String
certCAReferenceId	(Optional) Reference ID to input the certificate location. It is **mandatory** if certificateLocation is **ACM**. **Type**: String **Constraints**: The special characters allowed are ('=', '/', ',', '.', '@', '-').
certificateFileName	(Optional) A user defined file name for pushing the certificate into the AmazonELB device. It is **mandatory** if certificateLocation is **IAM**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the CA file name and intermediate certificate file name.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
Request payload if certificateLocation is ACM	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB (continued)

Name	Mandatory

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certCAReferenceId”: "arn:aws:iam::2313:amazonELB"
“certificateLocation”: "ACM"
“certificateType”: "PEM-.pem"
“pushRootAndIntermediateCertificates”: true
}
```

Request payload if certificateLocation is IAM

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateFileName: "sample.pem",
“certificateLocation”: "IAM",
“certificateType”: "PEM-.pem",
“pushRootAndIntermediateCertificates”: true
}
```

Certificate details for NginxPlus

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, and PEM-.cer
certificateLocation	(Mandatory) A user defined file name for pushing the certificate into the NginxPlus device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for NginxPlus (continued)

Name	Mandatory
	Type: String **Constraints**: The certificate file name should not begin and end with special characters except -, ., _. It should not be the same as CA file name and intermediate file name.
keyLocation	(Mandatory) A user defined file for pushing the key into the NginxPlus device. **Type**: String **Constraints**: The key file name should not begin and end with special characters except -, ., _. Key file name should be same as certificateFileName.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean

Request Payload

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateLocation":"/home/appviewx",
"keyLocation":"/home/appviewx",
"privateKeyInDevice": true
}
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the HAProxy device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean
privateKeyLocation	(Mandatory) A user defined file name for pushing the keys into the HAProxy device. It is **mandatory** if privateKeyInDevice is **true**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.

Request Payload

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateFileName":"/opt/haproxy/certificate_push.pem",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy (continued)

Name	Mandatory
"privateKeyLocation": true, "privateKeyLocation": "/opt/haproxy/test_cert.key" } }	

Response for Push and Bind SYNC API

Note: The response details/parameters are common for all vendor devices.

Parameters

Name	Description
response	Contains the parameters certificate, deviceProfiles, applicationConnectors, success and messages. **Type**: Object
certificate response	Details about the selected certificate which was used to push into the ADC devices **Type**: List <Object>
deviceProfiles response	Details about the device profiles to which the certificate is bound. **Type**: List <Object>
applicationConnectors response	Details about the application connectors where the push operation occurred. **Type**: List <Object>
success response	Determines whether the push operation succeeded. **Type**: Boolean
messages response	Details of the push operation. **Type**: List <String>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
message	Success or failure messages **Type**: String
appStatusCode	Application specific status code for the response. **Type**: String
tags	More info in case of failure response **Type**: Object
headers	Details of the response headers if any **Type**: Object

Sample Request/Response

Request Payload

```
{
 "applicationConnectorIds": [ "xx.xxx:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
 }
```

Note: Please refer to the "Request Structure" to identify the changeable values.

Response Details

```
{
 "response": {
 "certificate": <Selected Certificate>,
 "deviceProfiles": <Selected Profiles>,
 "applicationConnectors": <Application connectors with its work order status>,
 "success": <Status of the operation>,
 "messages": <Response message for the push action performed>
 },
 "message": null,
 "appStatusCode": <Error Code>,
 "tags": {},
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```


Sample Response (common for all vendors)


```
{
"response": {
"certificate": {
"commonName": "appviewx_test",
"serialNumber": "C4:DA:38:94:6B:A7:08:92:FB:A5:31:89:60:C6:D3:E7",
"issuerCommonName": "AppViewX Intermediate CA",
"status": "Managed",
"avxStatus": null,
"associatedObjects": [
"device_name::serverssl-insecure-compatible:Common:server-ssl"
],
"discoverySources": [
"device_name"
],
"subjectOrganization": "",
"subjectOrganizationUnit": "",
"subjectLocality": "",
"subjectState": "",
"subjectCountry": "",
"issuerOrganization": "AppViewX Inc",
"issuerOrganizationUnit": "",
"issuerLocality": "Seattle",
"issuerState": "Washington",
"issuerCountry": "US",
"version": "3",
"validFrom": 1617025560000,
"validTo": 1648561560000,
"validFor": "364 day(s) 23 hr(s) 57 min(s)",
"keyAlgorithmAndSize": "RSA 1024",
"signatureAlgorithm": "SHA160withRSA",
"signatureHashAlgorithm": "SHA160",
"keyUsage": "DigitalSignature, KeyEncipherment",
"extendedKeyUsage": "Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2) ",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"basicConstraints": "Subject Type=End entity, Path Length=none",
"group": "Default",
"subjectAlternativeNames": [
"DNS : appviewx_test"
],
"complianceStatus": "Compliant",
"applications": [],
"expiryStatus": "Valid",
"permission": null,
"category": "Server",
"uuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"id": "6061da0e92d28c50bd40336b",
"certificateAuthority": "AppViewX",
"authorityKeyIdentifier": "D0:D7:4B:D0:82:85:A4:98:70:6E:75:97:26:C6:A3:14:A5:C0:31:4D",
"subjectKeyIdentifier": "9D:1D:77:A0:CA:35:C5:5B:D4:3A:70:1A:AB:B0:2A:DD:CD:61:D9:80",
"issuerSerialNumber": "2C:F4:8E:5F:5F:D2:C2:F2:8A:DB:5A:D4:A1:06:A5:B2",
"authorityInfoAccess": [
"AuthorityInfoAccess : [ accessMethod : 1.3.6.1.5.5.7.48.1, alterativeName : , url :
https://172.18.0.157:31443/avxapi/controller/avxocsp?issuerserialnumber=597558399065138247098035107238630291 70 ]"
],
"certificatePolicies": [],
"crlDistributionPoints": [
"CrlDistributionPoint : [ name : , url : https://172.18.0.157:31443/avxapi/controller/avxcrl?crlFileName=597558399065138247098035107238630291 70.crl ]"
],
"thumbprintAlgorithm": "SHA-1",
"thumbPrint": "64:E8:0C:89:5F:6A:F1:2D:09:47:8C:5B:D5:DC:1B:CE:42:78:06:E7",
"type": "Others",
"genericFields": {
"vs_ip_AppViewX": "",
"device_name_AppViewX": ""
},
"certAttributes": {
"test": "test"
},
"validFromDate": null,
"validToDate": null,
"discoveredFileNames": [],
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

"issuingTemplate": null,

"csrGenerationSource": "appviewx",

"certificateHSMDetails": null,

"deviceDetails": null,

"newConnectors": [],

"csrAvailable": true,

"enhancedSANTypes": null,

"autoRenewDate": "",

"missingParamsForAutoRenew": "CSR parameters are available for certificate renewal",

"base64ImageContent": null,

"caConnectorName": null,

"caSettingName": null,

"suspendedCertificate": false,

"comments": null,

"mailAddress": "",

"streetAddress": "",

"postalCode": "",

"publicKeyModulus": null,

"requestIds": [

"R145",

"R146"

],

"orderId": null,

"publicKey":

"30:81:89:02:81:81:00:8E:EA:40:EF:61:06:00:89:9F:99:70:61:03:C3:D2:28:C1:EF:12:B2:FB:1A:6E:65:1C:85:3D:E1:8D:BD:DF:68:C9:76:A4:23:0D:79:A2:E6:52:F0:68:FC:AD:87:D2:D7:70:7C:76:C5:3F:A5:96:7B:D3:74:8A:5A:98:70:48:95:37:51:E3:33:1B:A7:32:19:E5:39:54:38:8A:1A:5B:A0:9C:5D:B5:D6:A6:EC:D9:DB:8A:FB:B8:BD:66:A6:E2:F9:D8:BF:AB:4D:F1:D3:31:E1:CB:6E:84:CF:C3:6F:E8:1F:E3:AF:12:F4:22:11:13:5E:F3:56:B1:8B:4E:18:BC:4D:02:03:01:00:01",

"ellipticCurve": null,

"issuedByRootCertificate": false,

"cumulativeSanCount": 1,

"privatekeyAvaliable": true

},

"deviceProfiles": [

{

"profileId": "device_name:@serverssl-insecure-compatible:@Common",

"vendor": "F5",

"deviceName": "device_name",

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"vendorCategory": "ADC",
"profileIdentifierForView": "device_name::serverssl-insecure-compatible:Common:server-ssl",
"profileDisplayOrder": "Partition:@Profile Name:@SSL Type",
"connectorType": "PROFILE_CONNECTOR",
"applications": [],
"hollisticViewData": {
"Partition": "Common",
"Profile Name": "serverssl-insecure-compatible",
"SSL Type": "server-ssl"
},
"overviewData": {},
"inventoryData": {
"associatedObjects": "device_name::serverssl-insecure-compatible:Common:server-ssl"
},
"vendorProperties": {
"partition": "Common",
"sslType": "server-ssl",
"name": "serverssl-insecure-compatible",
"partitionNameWithoutPath": "Common",
"iAppProfile": false
}
}
],
"applicationConnectors": [
{
"appconnectorId": "device_name:@serverssl-insecure-compatible:@Common:@9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"profileInfo": {
"profileId": "device_name:@serverssl-insecure-compatible:@Common",
"vendor": "F5",
"deviceName": "device_name",
"vendorCategory": "ADC",
"profileIdentifierForView": "device_name::serverssl-insecure-compatible:Common:server-ssl",
"profileDisplayOrder": "Partition:@Profile Name:@SSL Type",
"connectorType": "PROFILE_CONNECTOR",
"applications": [],
"hollisticViewData": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

"Partition": "Common",

"Profile Name": "serverssl-insecure-compatible",

"SSL Type": "server-ssl"

},

"overviewData": {},

"inventoryData": {

"associatedObjects": "device_name::serverssl-insecure-compatible:Common:server-ssl"

},

"vendorProperties": {

"partition": "Common",

"sslType": "server-ssl",

"certificateFileName": "certificate_push_202103291347.crt",

"rootCertificateFileName": "test_cert_ca.crt",

"certificatePartition": "Common",

"name": "serverssl-insecure-compatible",

"partitionNameWithoutPath": "Common",

"privateKeyPartition": "Common",

"keyType": "RSA",

"privateKeyFileName": "certificate_push_202103291347.key",

"iAppProfile": false

}

},

"backupInfo": {

"rollbackEligibility": false,

"backupDisplayMessage": null,

"backupCertUuid": null,

"backupCertCommonName": null,

"backupCertSerialNumber": null,

"unbindCertificate": false,

"backupProperties": null

},

"syncInfo": {

"syncMessage": {

"title": "Certificate Push",

"message": "Certificate pushed to the device successfully",

"utcTime": "2021-03-29T13:48:30.605",

"status": "SUCCESS",

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"batchId": null
},
"syncStatus": "SYNCRONIZED"
},
"userPreference": {
"autoPush": false,
"overwrite": true,
"securePush": false,
"userName": "admin",
"scheduledPushDate": null,
"modifiedData": true,
"modifiedTime": "2021-03-29T13:46:34.691",
"fileProperties": {
"pushRootAndIntermediateCertificates": false,
"certificateFileName": "certificate_push.crt",
"rootCertificateFileName": "test_cert_ca.crt",
"privateKeyFileName": "certificate_push.key"
},
"validationType": "DEFAULT",
"customApplications": null
},
"vendorScriptDetails": [],
"workflowDetails": {
"requestId": "146",
"workOrderId": "0",
"workflowStatus": "In Progress",
"workflowType": "VW",
"userName": "admin",
"actionType": "PUSHBIND",
"actionTypeDisplayName": "Push",
"taskId": "avxapi_5",
"taskName": "Post Push Script Execution",
"taskType": "others",
"taskStatus": "In Progress",
"currentAction": null,
"proceedProcess": null,
"breakdownProcess": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"reviewComponent": false,
"implemetationTime": 0,
"workOrderLogs": [
"Pre Push Script not available",
"Certificate push successful in device : device_name. Certificate/Key/CA file name already exists in device with different content. Certificate push has been completed successfully with names: [ Certificate File Name: certificate_push_202103291347.crt, Private Key File Name: certificate_push_202103291347.key, CA File Name: test_cert_ca.crt ]."
]
},
"loggerStatus": null,
"previousApplicationConnectorId": null
}
],
"success": true,
"messages": [
"Certificate push to the profiles completed successfully"
]
},
"message": null,
"appStatusCode": null,
"tags": {},
"headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push and Bind Certificate to ADC Profile

The API initiates a push of the certificate along with the private keys to the ADC devices and associates them to the device profiles.

Before You Begin

Ensure the following before attempting to push a certificate to a particular ADC device through AppViewX:

- ADC devices must be configured in AppViewX.
- The device should be in the Managed state.

Fetch Available Profiles API

Endpoint:	/certificate/profiles
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/profiles?category=ADC&vendor=F5&deviceName=F5_device&gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Details - Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
category *Query*	(Mandatory) Specifies the device category. **Type**: String **Possible values**: ADC, Server, and Firewall.
vendor *Query*	(Mandatory) Vendor for the chosen device. For example, **F5** is a vendor for the ADC category. **Type**: String **Possible values**: F5, Citrix, AVI, A10, AmazonELB, NginxPlus, and HAProxy.
certificateUuid	(Mandatory) Resource id of the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Details - Parameters (continued)

Name	Description
Query	**Type**: String **Constraints**: This can be obtained from search API.
deviceName	(Mandatory) Name of the device as per AppViewX Device Inventory.
Query	**Type**: String
inventory	(Mandatory) Name of AppViewX inventory where the certificate is present.
Query	**Type**: String **Possible values**: Server, Client, Code Signing, and Device.

Response Parameters

Name	Description
response	Contains the following response attributes for the fetch profiles request: objects, totalRecords, obtainedRecords, and obtainedRecordRange.
objects	List of available device profile Ids.
response	**Type**: List of String
totalRecords	Total number of profiles fetched.
response	**Type**: Integer
obtainedRecords	Total number of profiles fetched.
response	**Type**: Integer
obtainedRecordRange	Range of record found.
response	**Type**: Object
message	Success message of the action or failure description in case of error.
	Type: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Response


```
{
 "response": {
 "objects": [
 "device_name",
 "device_name:@apm-default-serverssl:@Common",
 "device_name:@clientssl-insecure-compatible:@Common",
 "device_name:@clientssl-secure:@Common",
 "device_name:@clientssl:@Common",
 "device_name:@crypto-client-default-serverssl:@Common",
 "device_name:@crypto-server-default-clientssl:@Common",
 "device_name:@pcoip-default-serverssl:@Common",
 "device_name:@serverssl-insecure-compatible:@Common",
 "device_name:@serverssl:@Common",
 "device_name:@splitsession-default-clientssl:@Common",
 "device_name:@splitsession-default-serverssl:@Common",
 "device_name:@wom-default-clientssl:@Common",
 "device_name:@wom-default-serverssl:@Common"
 ],
 "totalRecords": 14,
 "obtainedRecords": 14,
 "obtainedRecordRange": {
 "start": 0,
 "end": 0
 }
 },
 "message": "14 record(s) found",
 "appStatusCode": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Parameters (continued)

Name	Description
"tags": {}, "headers": null }	

Request Structure for Push and Bind ASYNC API

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	*https://<appviewx node ip>:<gateway port>/avxapi/certificate/pushToDevice?gwsource=external&gwkey=f000ca01*
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
certificateId	(Mandatory) Resource id of the certificate. **Type**: String **Constraint**: Optional if the Uuid of the certificate is present.
certificateUuid	(Optional) Certificate UUid **Type**: String **Constraint**: Mandatory only if certificateId is not present.
selectedProfiles	(Mandatory) ADC device profile id. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: These can be obtained from Fetch Available Profiles API • If a Profile connector is specified, then the certificate will be pushed and bound to the profile. • If a Default connector specified, then the certificate will be only pushed.
certificateDetails	(Mandatory) Certificate details for the server devices to be pushed. **Type**: Any of the following server devices: • Certificate details for F5 • Certificate details for Citrix • Certificate details for AVI • Certificate details for A10 • Certificate details for AmazonELB • Certificate details for NignixPlus • Certificate details for HAProxy

Certificate details for F5

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.crt
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into an F5 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into an F5 device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description
	Type: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
rootCertificateFileName	(Optional) A user defined file name for pushing the intermediate and root certificates into in a F5 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
"certificateId": "665efb67585b6b7259766f1b",
"selectedProfiles": ["F5:@shape-api-ssl:@Common"],
"certificateDetails": {
"certificateFileName": "F5testCert1.crt",
"certificateType": "PEM-.crt",
"privateKeyFileName": "F5testCert1.key",
"pushRootAndIntermediateCertificates": true,
"rootCertificateFileName": "test123_root.crt"
}
}
```

Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for F5 (continued)

Name	Description

{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}	

Certificate details for Citrix

Name	Description
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.crt, PEM-.cer, PEM-.pem, DER-.der, and DER-.cer
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the Citrix device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the Citrix device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description
	Type: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileName	(Optional) A user-defined file name for pushing the intermediate certificate into the Citrix device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the Citrix device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
"certificateUuid": "9eb94a53963d1ae326dbf4cda6077f55baa8476e",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for Citrix (continued)

Name	Description

"selectedProfiles": [

"device_name:@default:@sslvs"

],

"certificateDetails": {

"certificateFileName": "test123.crt",

"certificateKeyPairName": "test123",

"certificateType": "PEM-.crt",

"intermediateCertificateFileName": [

"test123_inter.crt"

],

"privateKeyFileName": "test123.key",

"pushRootAndIntermediateCertificates": true,

"rootCertificateFileName": "test123_root.crt",

"sniCert": "false",

"sniStatus": "false"

}

}

Response

{

"response": [

{

"requestId": "156",

"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"

}

],

"message": "1 connector(s) saved and push opertaion has been triggered.",

"appStatusCode": null,

"tags": {},

"headers": null

}

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the AVI device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the AVI device. **Type**: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
	Constraints: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.
rootCertificateFileName	(Optional) A user-defined file name for pushing the root certificate into the AVI device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Root file name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request Payload

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateType”:”PEM-.pem”,
 "certificateFileName":"certificate_push.pem",
 "privateKeyFileName":"certificate_push.key",
 "pushRootAndIntermediateCertificates": true,
 “intermediateCertificateFileNames”:[”test_cert_inter.crt”],
 "rootCertificateFileName": "test_cert_ca.crt"
 }
 }
```

Response

```
{
"response": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AVI (continued)

Name	Mandatory
{ "requestId": "156", "connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e" }], "message": "1 connector(s) saved and push opertaion has been triggered.", "appStatusCode": null, "tags": {}, "headers": null }	

Certificate details for A10

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, PEM-.cer, DER-.der, DER-.cer, PKCS#7-.p7b, PKCS#7-.p7c, PKCS#7-.p12, and PKCS#7-.pfx
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the A10 device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyFileName	(Mandatory) A user defined file name for pushing the keys into the A10 device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
	Type: String **Constraints**: The key file name should not begin or end with special characters except -, ., _. The key file name should be same as the certificateFileName.
pfxPassword	(Optional) Password for the **pfx** and **pkcs12** file type. It is **mandatory** only if the certificate file type is **.pfx** or **.pkcs12**. **Type**: Boolean **Constraints**: The password should be Base64 encoded.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean
intermediateCertificateFileNames	(Optional) A user-defined file name for pushing the intermediate certificate into the A10 device. It is **mandatory** if **pushRootAndIntermediateCertificates = true**. **Type**: String **Constraints**: Intermediate file or bundle name should not begin and end with special characters except -, _, .. It should not be the same as the certificate file name.

Request payload for non pfx and p12 cert types

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory

"device_name:@serverssl-insecure-compatible:@Common"

],

"certificateDetails":{

“certificateType”:”PEM-.crt”,

"certificateFileName":"certificate_push.crt",

"privateKeyFileName":"certificate_push.key",

"pushRootAndIntermediateCertificates": true,

"intermediateCertificateFileNames":["test_cert_ca.crt"]

}

}

Request payload for pfx and p12 cert types

{

"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",

"selectedProfiles":[

"device_name:@serverssl-insecure-compatible:@Common"

],

"certificateDetails":{

“certificateType”:”PKCS-.pfx”,

"certificateFileName":"certificate_push.pfx",

"pushRootAndIntermediateCertificates": true,

"intermediateCertificateFileNames":["test_cert_ca.crt"],

“pfxPassword”:”cGFzc3dvcmQ=”

}

}

Response

{

"response": [

{

"requestId": "156",

"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"

}

],

"message": "1 connector(s) saved and push opertaion has been triggered.",

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for A10 (continued)

Name	Mandatory
"appStatusCode": null, "tags": {}, "headers": null }	

Certificate details for AmazonELB

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateLocation	(Mandatory) Location of the certificate. Values are **ACM** or **IAM**. **Type**: String
certCAReferenceId	(Optional) Reference ID to input the certificate location. It is **mandatory** if certificateLocation is **ACM**. **Type**: String **Constraints**: The special characters allowed are ('=', '/', ',', '.', '@', '-').
certificateFileName	(Optional) A user defined file name for pushing the certificate into the AmazonELB device. It is **mandatory** if certificateLocation is **IAM**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB (continued)

Name	Mandatory
	from both the CA file name and intermediate certificate file name.
pushRootAndIntermediateCertificates	(Optional) Determines whether both Root and Intermediate certificate needs to be pushed. **Type**: Boolean

Request payload if certificateLocation is ACM

```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certCAReferenceId”: "arn:aws:iam::2313:amazonELB"
 “certificateLocation”: "ACM"
 “certificateType”: "PEM-.pem"
 “pushRootAndIntermediateCertificates”: true
 }
```

Request payload if certificateLocation is IAM

```
{
 "certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
 "selectedProfiles":[
 "device_name:@serverssl-insecure-compatible:@Common"
 ],
 "certificateDetails":{
 “certificateFileName: "sample.pem",
 “certificateLocation”: "IAM",
 “certificateType”: "PEM-.pem",
 “pushRootAndIntermediateCertificates”: true
 }
```

Response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for AmazonELB (continued)

Name	Mandatory

{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}	

Certificate details for NginxPlus

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem, PEM-.crt, and PEM-.cer
certificateLocation	(Mandatory) A user defined file name for pushing the certificate into the NginxPlus device. **Type**: String **Constraints**: The certificate file name should not begin and end with special characters except -, ., _. It should not be the same as CA file name and intermediate file name.
keyLocation	(Mandatory) A user defined file for pushing the key into the NginxPlus device. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for NginxPlus (continued)

Name	Mandatory
	Constraints: The key file name should not begin and end with special characters except -, ., _. Key file name should be same as certificateFileName.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean

Request Payload


```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateLocation":"/home/appviewx",
"keyLocation":"/home/appviewx",
"privateKeyInDevice": true
}
}
```


Response


```
{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
"tags": {},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for NginxPlus (continued)

Name	Mandatory
"headers": null }	

Certificate details for HAProxy

Name	Mandatory
certificateType	(Mandatory) Type of the certificate **Type**: String **Possible Certificate types**: PEM-.pem
certificateFileName	(Mandatory) A user defined file name for pushing the certificate into the HAProxy device. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.
privateKeyInDevice	(Optional) Determines whether private key needs to be pushed into the device. **Type**: Boolean
privateKeyLocation	(Mandatory) A user defined file name for pushing the keys into the HAProxy device. It is **mandatory** if privateKeyInDevice is **true**. **Type**: String **Constraints**: The certificate file name should not begin or end with special characters except -, ., _. The certificate file name should also be different from both the root and intermediate certificate file names.

Request Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate details for HAProxy (continued)

Name	Mandatory


```
{
"certificateUuid":"9eb94a53963d1ae326dbf4cda6077f55baa8476e",
"selectedProfiles":[
"device_name:@serverssl-insecure-compatible:@Common"
],
"certificateDetails":{
“certificateType”:”PEM-.pem”,
"certificateFileName":"/opt/haproxy/certificate_push.pem",
"privateKeyLocation": true,
"privateKeyLocation": "/opt/haproxy/test_cert.key"
}
}
```


Response


```
{
"response": [
{
"requestId": "156",
"connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
}
],
"message": "1 connector(s) saved and push opertaion has been triggered.",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Response Structure for Push and Bind ASYNC API

Note: The response details/parameters are common for all vendor devices.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters

Name	Description
response	Contains Request id and connector id. **Type**: Object
requestId response	Request Id for push action for the application connector. **Type**: String
connectorId response	Application connector Id. **Type**: String
message	Success or failure messages **Type**: String
appStatusCode	Application specific status code for the response. **Type**: String
tags	More info in case of failure response **Type**: Object
headers	Details of the response headers if any **Type**: Object

Sample Response (common for all vendors)


```
{
 "response": [
 {
 "requestId": "156",
 "connectorId": "device_name:@default:@clentssl:@9eb94a53963d1ae326dbf4cda6077f55baa8476e"
 }
 ],
 "message": "1 connector(s) saved and push opertaion has been triggered.",
 "appStatusCode": null,
 "tags": {},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Rollback Certificate to ADC profile

The API initiates the rollback of a certificate to an ADC profile.

Before you begin

Ensure the following before attempting to rollback certificate to a ADC device profile through AppViewX:

- ADC devices must be configured in AppViewX.
- The device should be in the Managed state

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Approval is not required:** Enable this mode by setting the 'Certificate Requests Need Approval?' flag to false in the Certificate Policy.
- **Approval is required**: If the approval setting in the policy cannot be changed, users can approve specific requests by following the After you are done section.

Request Structure

Endpoint:	/certificate/rollback
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/rollback?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Value of the parameter should be **'application/json'**
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
autoApproval *Query*	Indicates whether the auto-approval is needed for the action. **Type**: String **Constraint**: Value of the parameter should be **yes**.
Payload *Body*	Contains all the parameters to be sent in the request body for the post request. **Type**: Payload

Payload

Payload

Name	Description
applicationConnectorIds	(Mandatory) Application connector id. **Type**: List <String>

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the rollback request
requestId response	Request Id for rollback action for the application connector. **Type**: String
connectorId	Application connector Id.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
response	**Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
202 Accepted	NA	App connector rollback action initiated for 1 connector(s).
202 Accepted	NA	Operation cannot be completed for one or more devices as the 'Resource' allocated to you does not have write permission. **Remediation**: Ensure that users have access to the device.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
400 Bad Request	MANDATORY_FIELD_MISSING	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	FIELD_VALUE_INVALID	Invalid value - <<field name>> **Remediation**: Ensure that a valid value is provided for the <<field name>> field in the request.
417 Expectation failed	CERT-APP-0012	Application connector ids cannot be empty. **Remediation**: Please provide value for the field applicationConnectorIds.
417 Expectation failed	ERR_APPLICATION_CONNECTOR_LIST_RETRIVAL	Unable to retrieve connector information. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_APP_CONNECTORS_NOT_FOUND	Application connector(s) not found. **Remediation**: Connector may not be available. Please provide correct value for the field applicationConnectorIds.
417 Expectation failed	ERR_INITIALIZE_ROLLBACK_REQUEST	Unable to initialize rollback request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
417 Expectation failed	ERR_ROLLBACK_INELIGIBLE	Push not triggered or succeeded or No existing data available for backup process **Remediation**: Push and bind certificate before rollback.
500 Internal Server Error	avx-common-011	Error while processing

Sample Request/Response

Request Payload


```
{
 "applicationConnectorIds": [ "device_name:@clientssl-insecure-compatible:@Common:@c46ec8a04da701721159ce0c3cf772367ade58cb" ]
 }
```


Response


```
{
"response": [
{
"requestId": "243",
"connectorId": "F5:@crypto-client-default-serverssl:@Common:@134c5c3a64ed8cf4e02cf32078ee1e2ffc1b109b"
}
],
"message": "App connector rollback action initiated for 1 connector(s).",
"appStatusCode": null,
"tags": {},
"headers": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

MultiCloud API

- Push Certificates to ACM
- Push Certificates to IAM
- Push Certificates to ELB via ACM
- Push Certificates to ELB via IAM
- Push Certificates to Cloudfront via ACM
- Push Certificates to Cloudfront via IAM
- Push Certificates to Azure Key Vault (Certificate Location)
- Push Certificates to Azure Key Vault (Secrets Location)
- Push Certificates to Azure Application Gateway (Gateway Listener Profile | Direct upload to Application Gateway)
- Push Certificates to Azure Application Gateway (Gateway Listener Profile | Choose from Key Vault)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Push Certificates to Azure Application Gateway (Gateway SSL Profile)
- Push Certificates to Azure App Service
- Push Certificates to Azure Enterprise Application Service
- Push Certificates to Azure App Registration Service
- Push Certificates to Azure API Management Service
- Push Certificates to GCP Certificate Manager Service (Scope: Global)
- Push Certificates to GCP Certificate Manager Service (Scope: Regional)
- Push Certificates to GCP Classic Certificates Service (Scope: Global)
- Push Certificates to GCP Classic Certificates Service (Scope: Regional)
- Push Certificates to GCP Load Balancer Service (via Classic Certificates)
- Push Certificates to GCP Load Balancer Service (via Certificate Manager-Global External LB)
- Push Certificates to GCP Load Balancer Service (via Certificate Manager-Regional Internal LB)

Push Certificates to ACM

This API will push certificates and their corresponding private keys to AWS devices with the AWS Certificate Manager (ACM) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the ACM service through AppViewX, ensure the following:

- AWS devices with the ACM service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible values**: ACM
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::acm",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"ACM",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"ACM",
  "certificateTags":{
  },
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "intermediateCertificateFileName":[
  ]
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@ACM"],
 "validationSettings":{
 }
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
   "headers": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to IAM

This API will push certificates and their corresponding private keys to AWS devices with the Identity Access and Management (IAM) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the IAM service through AppViewX, ensure the following:

- AWS devices with the IAM service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
	Type: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: IAM
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Possible Values: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::iam",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "certificateType":"PEM-.pem",
    "locationType":"IAM",
    "certificateFileName":"",
    "certCAReferenceId":"",
    "pushRootAndIntermediateCertificates":true,
    "defaultCertificate":false,
    "profileFilterSelection":"IAM",
    "certificateTags":{
    }
   },
  "certificateTags":{
  },
  "pushDetails":{
    "scriptLocation":"appviewx",
    "preValidationScriptPath":"",
    "postValidationScriptPath":"",
    "pushAutomatically":false
  },
  "certificateId":"661dbddf4c274a5eed7f5735",
  "selectedProfiles":[
    "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@IAM"],
}
```


Sample Response


```
{
    "response": [
        {
            "requestId": "51",
            "connectorId": "1715213308394"
        }
    ],
    "message": "1 connector(s) saved and push opertaion has been triggered.",
    "appStatusCode": null,
    "tags": {
    },
    "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to ELB via ACM

This API will push certificates and their corresponding private keys to AWS devices with the Elastic Load Balancer (ELB) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the ELB service through AppViewX, ensure the following:

- AWS devices with the ELB service should be added in AppViewX
- The devices should be in **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible values: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::elb",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"ELB",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"ELB",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@ELB"],
}
```

Sample Response

```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
   "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to ELB via IAM

This API will push certificates and their corresponding private keys to AWS devices with the Elastic Load Balancer (ELB) service.

Before You Begin

Before attempting to push a certificate to an AWS device with the ELB service through AppViewX, ensure the following:

- AWS devices with the ELB service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId	(Mandatory) Session ID received after login.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
 "generalInformation":{
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::elb",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"ELB",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"ELB",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@ELB"],
}
```


Sample Response


```
{
  "response": [
    {
      "requestId": "51",
      "connectorId": "1715213308394"
    }
  ],
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "message": "1 connector(s) saved and push opertaion has been triggered.",
  "appStatusCode": null,
  "tags": {
  },
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Cloudfront via ACM

This API will push certificates and their corresponding private keys to AWS devices with the CloudFront service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before You Begin

Before attempting to push a certificate to an AWS device with the CloudFront service through AppViewX, ensure the following:

- AWS devices with the CloudFront service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible values**: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation":{
    "category":"cloud",
    "vendor":"AWS",
    "profileFilterSelection":"::cloudfront",
    "name":"AWS connector",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"CloudFront",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"CloudFront",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@CloudFront"],
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Cloudfront via IAM

This API will push certificates and their corresponding private keys to AWS devices with the CloudFront service.

Before You Begin

Before attempting to push a certificate to an AWS device with the CloudFront service through AppViewX, ensure the following:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- AWS devices with the CloudFront service should be added in AppViewX
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login. **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	(Mandatory) AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	(Mandatory) AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	(Mandatory) Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation

Name	Description
category	(Mandatory) Type of the target system to which the certificate will be pushed **Type**: String **Possible values**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible values**: AWS
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible values**: ELB
name	Name of the connector that will be created to push the certificate to the cloud device **Type**: String
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible values: Server, Client, Code signing
locationType	(Optional) Location where the certificate will be stored **Type**: String
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certCAReferenceId	(Mandatory) ID of the issuing Certificate Authority **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible values**: • 1: Yes • 0: No
defaultCertificate	(Mandatory) Name of the default certificate that will be used as a fallback option This certificate will be pushed in the event that the intended certificate cannot be pushed.
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file **Type**: String **Possible Values**: **In AppViewX** and **In Device**
preValidationScriptPath	(Optional) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Optional) Location of the script that will be executed after the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible values**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
417 Expectation failed	**FIELD_VALUE_INVALID**	Cooling period should be 0 or greater than 1 **Possible remediation**: Please provide the correct value in the field **coolingPeriod**.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation":{
  "category":"cloud",
  "vendor":"AWS",
  "profileFilterSelection":"::cloudfront",
  "name":"AWS connector",
  "description":""
 },
 "certificateDetails":{
  "certificateType":"PEM-.pem",
  "locationType":"CloudFront",
  "certificateFileName":"",
  "certCAReferenceId":"",
  "pushRootAndIntermediateCertificates":true,
  "defaultCertificate":false,
  "profileFilterSelection":"CloudFront",
  "certificateTags":{
  }
 },
 "certificateTags":{
 },
 "pushDetails":{
  "scriptLocation":"appviewx",
  "preValidationScriptPath":"",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "postValidationScriptPath":"",
  "pushAutomatically":false
 },
 "certificateId":"661dbddf4c274a5eed7f5735",
 "selectedProfiles":[
  "AWS:@mctest:@xxx:@AppViewX:@US East (N. Virginia):@CloudFront"],
}
```

Sample Response

```
{
   "response": [
      {
         "requestId": "51",
         "connectorId": "1715213308394"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {
   },
   "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure Key Vault (Certificate Location)

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the Key Vault service.

Before You Begin

Before attempting to push a certificate to a Azure device with the key vault service through AppViewX, ensure the following:

- Azure devices with the key vault service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Key vault

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
name	(Mandatory) Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	(Optional) Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certificateLocation	(Optional) Key vault location where the certificate will be stored **Type**: String **Possible value(s)**: certificate
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: Boolean **Possible value(s)**: • 1: Yes • 0: No
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
  "generalInformation": {
    "category": "cloud",
    "vendor": "Azure",
    "serviceFilterSelection": "Key vault",
    "name": "Azure connector",
    "description": "",
    "profileType": "Push and Bind Profiles"
  },
  "certificateDetails": {
    "certificateType": "PKCS12-.p12",
    "certificateFileName": "kv10cert.p12",
    "certificateLocation": "certificates",
    "pushRootAndIntermediateCertificates": true,
    "certificateTags": {

    }
  },
  "pushDetails": {
    "scriptLocation": "appviewx",
    "preValidationScriptPath": "",
    "postValidationScriptPath": "",
    "pushAutomatically": false
  },
  "certificateId": "67a9a1535e121f50b46791d0",
  "selectedProfiles": [
    "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.KeyVault/vaults::eastus::multicloud::multicloud-kv"
  ]
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample Response


```
{
   "response": [
      {
         "requestId": "353",
         "connectorId": "1739267357850"
      }
   ],
   "message": "1 connector(s) saved and push operation has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure Key Vault (Secrets Location)

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the key vault service.

Before You Begin

Before attempting to push a certificate to a Azure device with the key vault service through AppViewX, ensure the following:

- Azure devices with the key vault service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username	AppViewX login username

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Key vault
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
certificateLocation	(Optional) Key vault location where the certificate will be stored **Type**: String **Possible value(s)**: secrets
secretCertificateEnabled	(Optional) Enable certificate after it is pushed to the target system **Type**: Boolean **Possible value(s)**: true, false
setActivationDate	(Optional) Specify if an activation date has to be set for the certificate being pushed **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): true, false
secretCertificateActivationDate	(Mandatory if **setActivationDate** = **true**) Activation date of the certificate **Type**: Long
activationTimezone	(Mandatory if **setActivationDate** = **true**) Time zone of the activation date of the certificate **Type**: String
setExpirationDate	(Optional) Specify if an expiration date has to be set for the certificate being pushed **Type**: String **Possible value(s)**: true, false
secretCertificateExpiry	(Mandatory if **setExpirationDate** = **true**) Expiration date of the certificate **Type**: Long
expirationTimezone	(Mandatory if **setActivationDate** = **true**) Time zone of the expiration date of the certificate **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "Key vault",
  "name": "Azure connector2",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PKCS12-.p12",
  "certificateFileName": "kv10sec.p12",
  "certificateLocation": "secrets",
  "secretCertificateEnabled": true,
  "setActivationDate": true,
  "secretCertificateActivationDate": 1739190546000,
  "activationTimezone": "GMT",
  "setExpirationDate": true,
  "secretCertificateExpiry": 1740745746000,
  "expirationTimezone": "GMT",
  "pushRootAndIntermediateCertificates": true,
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9a1535e121f50b46791d0",
 "selectedProfiles": [
  "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.KeyVault/vaults::eastus::multicloud::multicloud-kv"
 ]
}
```


Sample Response


```
{
  "response": [
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    {
      "requestId": "354",
      "connectorId": "1739342741168"
    }
  ],
  "message": "1 connector(s) saved and push operation has been triggered.",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Push Certificates to Azure Application Gateway (Gateway Listener Profile | Direct upload to Application Gateway)

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the application gateway service.

Before You Begin

Before attempting to push a certificate to a Azure device with the application gateway service through AppViewX, ensure the following:

- Azure devices with the application gateway service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Application Gateway
profileFilterSelection	Target profile that defines the details for integrating and pushing certificates to the target system **Type**: String **Possible value(s)**: **::Listener**
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
pushLocation	(Mandatory) Endpoint where the certificate will be pushed **Type**: String **Possible value(s)**: Application Gateway
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: Boolean **Possible value(s)**: • 1: Yes • 0: No
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: Gateway Listener Profile
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "Application Gateway",
  "profileFilterSelection": "::Listener",
  "name": "Azure connector3",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PKCS12-.p12",
  "certificateFileName": "cert10ag.p12",
  "isNewCertificate": true,
  "pushLocation": "Application Gateway",
  "pushRootAndIntermediateCertificates": true,
  "profileFilterSelection": "Gateway Listener Profile",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "postValidationScriptPath": "",
    "pushAutomatically": false
  },
  "certificateId": "67a9a1535e121f50b46791d0",
  "selectedProfiles": [

 "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.Network/applicationGateways::v2::eastus::multicloud::
TestAG::Listener::Test-L01::443"
  ]
}
```


Sample Response


```
{
    "response": [
        {
            "requestId": "355",
            "connectorId":
 "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.Network/applicationGateways::v2::eastus::multicloud::
TestAG::Listener::Test-L01::443:@a188f63b41cc837887ad9104b121099277fcbfef"
        }
    ],
    "message": "1 connector(s) saved and push opertaion has been triggered.",
    "appStatusCode": null,
    "tags": {},
    "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure Application Gateway (Gateway Listener Profile | Choose from Key Vault)

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the application gateway service.

Before You Begin

Before attempting to push a certificate to a Azure device with the application gateway service through AppViewX, ensure the following:

- Azure devices with the application gateway service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Possible value(s): Application Gateway
profileFilterSelection	Target profile that defines the details for integrating and pushing certificates to the target system **Type**: String **Possible value(s)**: **::Listener**
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed to the gateway **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
isNewCertificate	(Optional) Specify if the certificate being pushed to the application gateway is a new certificate or an existing certificate that is being replaced **Type**: String **Possible value(s)**: true, false
pushLocation	(Mandatory) Endpoint where the certificate will be pushed **Type**: String **Possible value(s)**: Application Gateway
keyVaultSubscriptionId	(Optional) Subscription ID of the key vault in which the certificate will stored after it is pushed **Type**: String
keyVaultName	(Optional) Name of the key vault in which the certificate will stored after it is pushed **Type**: String
useExisting	(Optional) Specify if the certificate being pushed to the key vault needs to be replaced **Type**: String **Possible value(s)**: true, false
keyVaultCertificateName	(Optional) Name assigned to the certificate after it is pushed to the key vault **Type**: String
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): • 1: Yes • 0: No
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: Gateway Listener Profile
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "Application Gateway",
  "profileFilterSelection": "::Listener",
  "name": "Azure connector4",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PKCS12-.p12",
  "certificateFileName": "certagviakv.p12",
  "isNewCertificate": true,
  "pushLocation": "Key vault",
  "keyVaultSubscriptionId": "0c740e00-404f-44f7-807a-416d671de225",
  "keyVaultName": "multicloud-kv",
  "useExisting": false,
  "keyVaultCertificateName": "newkv10",
  "pushRootAndIntermediateCertificates": true,
  "profileFilterSelection": "Gateway Listener Profile",
  "certificateTags": {

  }
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9a1535e121f50b46791d0",
 "selectedProfiles": [

"Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.Network/applicationGateways::v2::eastus::multicloud::
TestAG::Listener"
 ]
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "357",
         "connectorId": "1739492235630"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **HostName**: A human-readable label assigned to a device (host) on a network

  The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure Application Gateway (Gateway SSL Profile)

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the application gateway service.

Before You Begin

Before attempting to push a certificate to a Azure device with the application gateway service through AppViewX, ensure the following:

- Azure devices with the application gateway service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Headers
Content-Type: application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible value(s)**: Application Gateway
profileFilterSelection	Target profile that defines the details for integrating and pushing certificates to the target system **Type**: String **Possible value(s)**: **::SslProfile**
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String
isNewCertificate	(Optional) Specify if the certificate being pushed to the application gateway is a new certificate or an existing certificate that is being replaced **Type**: String **Possible value(s)**: true, false
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: Gateway SSL Profile
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
    "category": "cloud",
    "vendor": "Azure",
    "serviceFilterSelection": "Application Gateway",
    "profileFilterSelection": "::SslProfile",
    "name": "Azure connector",
    "description": "",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "profileType": "Push and Bind Profiles"
  },
  "certificateDetails": {
    "certificateType": "DER-.cer",
    "certificateFileName": "gw10ssl.cer",
    "isNewCertificate": true,
    "pushRootAndIntermediateCertificates": true,
    "profileFilterSelection": "Gateway SSL Profile",
    "certificateTags": {

    }
  },
  "pushDetails": {
    "scriptLocation": "appviewx",
    "preValidationScriptPath": "",
    "postValidationScriptPath": "",
    "pushAutomatically": false
  },
  "certificateId": "67a25fc32ab5e845a7ca9e86",
  "selectedProfiles": [

 "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.Network/applicationGateways::v2::eastus::multicloud::
TestAG::SslProfile::TestSSL"
  ]
}
```


Sample Response


```
{
    "response": [
        {
            "requestId": "358",
            "connectorId":
 "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.Network/applicationGateways::v2::eastus::multicloud::
TestAG::SslProfile::TestSSL:@231e7ec446bd31d5883eaaeef20033687910e884"
        }
    ],
    "message": "1 connector(s) saved and push operation has been triggered.",
    "appStatusCode": null,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "tags": {},
  "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure App Service

This API will push certificates and their corresponding private keys to Microsoft Azure devices with app service.

Before You Begin

Before attempting to push a certificate to a Azure device with app service through AppViewX, ensure the following:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Azure devices with app service should be added in AppViewX.
• The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource	Source from which the request is triggered. (E.g. external)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Query	**Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: App Service
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed to the app service is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
pushLocation	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: App Service
sslState	(Optional) SSL configuration for binding certificate to a domain **Type**: String **Possible value(s)**: SNI Enabled, IP Based Enables, Disabled
restartRequired	(optional) Specify if app service needs to be restarted after the certificate is pushed **Type**: Boolean **Possible value(s)**: true, false
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
locationType	(Mandatory) Profile type for pushing the certificate to the app service **Type**: String **Possible value(s)**: PFX, CER

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Possible value(s): • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "App Service",
  "name": "Azure connector5",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PKCS12-.p12",
  "certificateFileName": "certappser10.p12",
  "isNewCertificate": true,
  "pushLocation": "App Service",
  "pushRootAndIntermediateCertificates": true,
  "certificateTags": {

  },
  "locationType": "PFX"
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9a1535e121f50b46791d0",
 "selectedProfiles": [
  "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.Web/sites::Basic::East US::multicloud::TestMC11"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 ]
}
```

Sample Response

```
{
   "response": [
      {
         "requestId": "359",
         "connectorId": "1739922695709"
      }
   ],
   "message": "1 connector(s) saved and push operation has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure Enterprise Application Service

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the enterprise application service.

Before You Begin

Before attempting to push a certificate to a Azure device with the enterprise application service through AppViewX, ensure the following:

- Azure devices with the enterprise application service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username	AppViewX login username

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Enterprise Application
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible value(s)**: push and bind profiles, push only profiles
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
isActive	(Optional) Specify if the certificate being pushed should be made the active certificate for the enterprise application service. **Type**: String **Possible value(s)**: true, false
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String
additionalNotificationEmailAddress(s)	(Optional) Additional email addresses that should be notified when the certificate is pushed and/or made active **Type**: String
defaultNotificationEmailAddress	(Optional) Default email addresses that should be notified when the certificate is pushed and/or made active

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "Enterprise Application",
  "name": "Azure connector6",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PKCS12-.pfx",
  "isActive": true,
  "certificateTags": {

  },
  "additionalNotificationEmailAddress": [

  ],
  "defaultNotificationEmailAddress": [
   "abc@xyz.com",
   "pqr@xyz.com"
  ]
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9a1535e121f50b46791d0",
 "selectedProfiles": [
  "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::Microsoft.EnterpriseApplication/sso::MCTest::5921614e-69a4-40d5-a814-0359e3a56a63"
 ]
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "360",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "connectorId":
 "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::Microsoft.EnterpriseApplication/sso::MCTest::5921614e-69a4-40d5-a814-0359e3a56a63:@a188f63b41cc
837887ad9104b121099277fcbfef"
      }
  ],
  "message": "1 connector(s) saved and push opertaion has been triggered.",
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Push Certificates to Azure App Registration Service

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the app registration service.

Before You Begin

Before attempting to push a certificate to a Azure device with the app registration service through AppViewX, ensure the following:

- Azure devices with the app registration service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password	AppViewX login password

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: App Registration
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind profiles, push only profiles
description	Additional details related to the certificate being pushed, the connector for pushing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "App Registration",
  "name": "Azure connector7",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PEM-.cer",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9a1535e121f50b46791d0",
 "selectedProfiles": [
  "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::Microsoft.AppRegistration/app::MCTest::5921614e-69a4-40d5-a814-0359e3a56a63"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 ]
}
```

Sample Response

```
{
   "response": [
      {
         "requestId": "361",
         "connectorId": "1741248739433"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to Azure API Management Service

This API will push certificates and their corresponding private keys to Microsoft Azure devices with the API management service.

Before You Begin

Before attempting to push a certificate to a Azure device with the API management service through AppViewX, ensure the following:

- Azure devices with the API management service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username	AppViewX login username

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
serviceFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Application Gateway
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateType	(Mandatory) Type of the certificate that is being pushed **Type**: String **Possible value(s)**: Server, Client, Code signing
certificateFileName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
pushLocation	(Mandatory) Endpoint where the certificate will be pushed **Type**: String **Possible value(s)**: Application Gateway
pushRootAndIntermediateCertificates	(Optional) Push root and intermediate certificates along with the end certificate **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): • 1: Yes • 0: No
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Possible value(s): • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "Azure",
  "serviceFilterSelection": "Api Management",
  "name": "Azure connector8",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateType": "PKCS12-.p12",
  "certificateFileName": "certapim10.p12",
  "isNewCertificate": true,
  "pushLocation": "Api Management",
  "sslState": "SniEnabled",
  "restartRequired": false,
  "pushRootAndIntermediateCertificates": true,
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9a1535e121f50b46791d0",
 "selectedProfiles": [
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
   "Azure.All::e5f90d85-3cdf-457d-a611-1aca82b0843b::0c740e00-404f-44f7-807a-416d671de225::Microsoft.ApiManagement/service::East
 US::multicloud::TestMC1"
 ]
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "362",
         "connectorId": "1739481326139"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Certificate Manager Service (Scope: Global)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the certificate manager service.

Before You Begin

Before attempting to push a certificate to a GCP device with the certificate manager service through AppViewX, ensure the following:

- GCP devices with the certificate manager service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
	Constraints: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Certificate Manager
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
region	(Optional) Scope of the certificate being pushed **Type**: String **Possible value(s)**: • Global (Certificate is available for use across all regions within a GCP project) • Regional (Certificate is limited to a specific region within a GCP project)
certificateDescription	(Optional) Additional details related to the certificate being pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: Certificate Manager
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Type: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "GCP",
  "profileFilterSelection": ":Certificate Manager",
  "name": "GCP connector",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "isNewCertificate": true,
  "certificateName": "feb10cm2",
  "region": "global",
  "certificateDescription": "",
  "profileFilterSelection": "Certificate Manager",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9f5ce2ff94729fda605ac",
 "selectedProfiles": [
  "GCP.Single.All:pm-project-lab-1-391708:Certificate Manager"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 ]
}
```

Sample Response


```
{
   "response": [
      {
         "requestId": "364",
         "connectorId": "1741334777227"
      }
   ],
   "message": "1 connector(s) saved and push operation has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Certificate Manager Service (Scope: Regional)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the certificate manager service.

Before You Begin

Before attempting to push a certificate to a GCP device with the certificate manager service through AppViewX, ensure the following:

- GCP devices with the certificate manager service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username	AppViewX login username

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Certificate Manager
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Type: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
region	(Optional) Scope of the certificate being pushed **Type**: String **Possible value(s)**: • Global (Certificate is available for use across all regions within a GCP project) • Regional (Certificate is limited to a specific region within a GCP project)
certificateDescription	(Optional) Additional details related to the certificate being pushed **Type**: String
profileFilterSelection	Specific profile type where the certificate will be applied

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String **Possible value(s)**: Certificate Manager
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Possible value(s): • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "GCP",
  "profileFilterSelection": ":Certificate Manager",
  "name": "GCP connector",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "isNewCertificate": true,
  "certificateName": "cmreg10",
  "region": "us-east1",
  "certificateDescription": "",
  "profileFilterSelection": "Certificate Manager",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9f5ce2ff94729fda605ac",
 "selectedProfiles": [
  "GCP.Single.All:pm-project-lab-1-391708:Certificate Manager"
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 ]
}
```

Sample Response

```
{
   "response": [
      {
         "requestId": "365",
         "connectorId": "1740522308007"
      }
   ],
   "message": "1 connector(s) saved and push operation has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Classic Certificates Service (Scope: Global)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the classic certificates service.

Before You Begin

Before attempting to push a certificate to a GCP device with the classic certificates service through AppViewX, ensure the following:

- GCP devices with the classic certificates service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username	AppViewX login username

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Header	**Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Classic Certificates
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Possible value(s): push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
region	(Optional) Scope of the certificate being pushed **Type**: String **Possible value(s)**: • Global (Certificate is available for use across all regions within a GCP project) • Regional (Certificate is limited to a specific region within a GCP project)
certificateDescription	(Optional) Additional details related to the certificate being pushed **Type**: String
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): Classic Certificates
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "category": "cloud",
  "vendor": "GCP",
  "profileFilterSelection": ":Classic Certificates",
  "name": "GCP connector2",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "isNewCertificate": true,
  "certificateName": "feb10cc",
  "region": "global",
  "certificateDescription": "",
  "profileFilterSelection": "Classic Certificates",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9f5ce2ff94729fda605ac",
 "selectedProfiles": [
  "GCP.Single.All:pm-project-lab-1-391708:Classic Certificates"
 ]
}
```


Sample Response


```
{
  "response": [
    {
      "requestId": "366",
      "connectorId": "1739655195702"
    }
  ],
  "message": "1 connector(s) saved and push operation has been triggered.",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "appStatusCode": null,
  "tags": {},
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Classic Certificates Service (Scope: Regional)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the classic certificates service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before You Begin

Before attempting to push a certificate to a GCP device with the classic certificates service through AppViewX, ensure the following:

- GCP devices with the classic certificates service should be added in AppViewX.
- The devices should be in **Managed** state.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String **Possible value(s)**: Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: Classic Certificates
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateName	(Mandatory) Name of the certificate being pushed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Type: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
region	(Optional) Scope of the certificate being pushed **Type**: String **Possible value(s)**: • Global (Certificate is available for use across all regions within a GCP project) • Regional (Certificate is limited to a specific region within a GCP project)
certificateDescription	(Optional) Additional details related to the certificate being pushed **Type**: String
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: Classic Certificates
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
    "category": "cloud",
    "vendor": "GCP",
    "profileFilterSelection": ":Classic Certificates",
    "name": "GCP connector2",
    "description": "",
    "profileType": "Push and Bind Profiles"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 },
 "certificateDetails": {
  "isNewCertificate": true,
  "certificateName": "feb10cc",
  "region": "us-east1",
  "certificateDescription": "",
  "profileFilterSelection": "Classic Certificates",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9f5ce2ff94729fda605ac",
 "selectedProfiles": [
  "GCP.Single.All:pm-project-lab-1-391708:Classic Certificates"
 ]
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "366",
         "connectorId": "1739655195702"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Load Balancer Service (via Classic Certificates)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the load balancer service.

Before You Begin

Before attempting to push a certificate to a GCP device with the load balancer service through AppViewX, ensure the following:

- GCP devices with the load balancer service should be added in AppViewX.
- The devices should be in **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Possible value(s): Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: Azure
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: LB
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateLocation	(Mandatory) Certificate upload location **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): • Classic Certificates (Upload your certificate and private key directly to the load balancer's configuration.) • Certificate Manager (Reference certificates managed by Certificate Manager in your load balancer configuration.)
certificateName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
certificateDescription	(Optional) Additional details related to the certificate being pushed **Type**: String
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: LB
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
    "category": "cloud",
    "vendor": "GCP",
    "profileFilterSelection": ":LB",
    "name": "GCP connector3",
    "description": "",
    "profileType": "Push and Bind Profiles"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 },
 "certificateDetails": {
  "certificateLocation": "Classic Certificates",
  "isNewCertificate": true,
  "certificateName": "feb10lb-cc",
  "certificateDescription": "",
  "profileFilterSelection": "Load Balancer",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9f5ce2ff94729fda605ac",
 "selectedProfiles": [
  "GCP.Single.All:pm-project-lab-1-391708:global:nw-lb:Network:nw-lb-target-proxy:targetSslProxy:LB"
 ]
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "367",
         "connectorId":
 "GCP.Single.All:pm-project-lab-1-391708:global:nw-lb:Network:nw-lb-target-proxy:targetSslProxy:LB:@026e4051353bb9f88e0289d9d6ecb2e3d115b835"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Load Balancer Service (via Certificate Manager-Global External LB)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the load balancer service.

Before You Begin

Before attempting to push a certificate to a GCP device with the load balancer service through AppViewX, ensure the following:

- GCP devices with the load balancer service should be added in AppViewX.
- The devices should be in **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Possible value(s): Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: GCP
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: LB
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateLocation	(Mandatory) Certificate upload location **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): • Classic Certificates (Upload your certificate and private key directly to the load balancer's configuration.) • Certificate Manager (Reference certificates managed by Certificate Manager in your load balancer configuration.)
certificateName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
certificateDescription	(Optional) Additional details related to the certificate being pushed **Type**: String
isNewCertificateMap	(Mandatory) Specify if a new certificate map needs to be created. A certificate map is an organized listing of one or more certificate map entries. **Type**: Boolean **Possible value(s)**: true, false
isNewCertificateMapEntry	(Mandatory) Specify if a new certificate map entry needs to be created. A certificate map entry is an individual entry in the certificate map that associates a domain name with a SSL/TLS certificate. **Type**: Boolean **Possible value(s)**: true, false

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
isPrimaryCertificateMapEntry	(Mandatory) Specify if the selected certificate map entry needs to be made primary. **Type**: Boolean **Possible value(s)**: true, false
certificateMapName	(Mandatory) Name for the certificate map **Type**: String
certificateMapEntryName	(Mandatory) Individual map entry value to be listed in the certificate map **Type**: String
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: Load Balancer
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file. Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error **Type**: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>> **Possible remediation**: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request


```
{
 "generalInformation": {
  "category": "cloud",
  "vendor": "GCP",
  "profileFilterSelection": ":LB",
  "name": "GCP connector4",
  "description": "",
  "profileType": "Push and Bind Profiles"
 },
 "certificateDetails": {
  "certificateLocation": "Certificate Manager",
  "isNewCertificate": true,
  "certificateName": "lb10cn",
  "certificateDescription": "",
  "isNewCertificateMap": true,
  "isNewCertificateMapEntry": true,
  "isPrimaryCertificateMapEntry": true,
  "profileFilterSelection": "Load Balancer",
  "certificateTags": {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    },
    "certificateMapName": "cmn10",
    "certificateMapEntryName": "cmen10"
  },
  "pushDetails": {
    "scriptLocation": "appviewx",
    "preValidationScriptPath": "",
    "postValidationScriptPath": "",
    "pushAutomatically": false
  },
  "certificateId": "67a9f5ce2ff94729fda605ac",
  "selectedProfiles": [
    "GCP.Single.All:pm-project-lab-1-391708:global:psr-url-map-1:Application:psr-url-map-1-target-proxy:targetHttpsProxy:LB"
  ]
}
```


Sample Response


```
{
    "response": [
        {
            "requestId": "368",
            "connectorId":
 "GCP.Single.All:pm-project-lab-1-391708:global:psr-url-map-1:Application:psr-url-map-1-target-proxy:targetHttpsProxy:LB:@026e4051353bb9f88e0289d9d6ecb
2e3d115b835"
        }
    ],
    "message": "1 connector(s) saved and push opertaion has been triggered.",
    "appStatusCode": null,
    "tags": {},
    "headers": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Push Certificates to GCP Load Balancer Service (via Certificate Manager-Regional Internal LB)

This API will push certificates and their corresponding private keys to Google Cloud Platform (GCP) devices with the load balancer service.

Before You Begin

Before attempting to push a certificate to a GCP device with the load balancer service through AppViewX, ensure the following:

- GCP devices with the load balancer service should be added in AppViewX.
- The devices should be in **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/pushToDevice
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/pushToDevice?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Request Parameters

Name	Description
sessionId *Header*	(Mandatory) Session ID received after login **Type**: String **Constraints**: Required if **username** and **password** are not provided.
username *Header*	AppViewX login username **Type**: String **Constraints**: Required if **sessionId** is not provided.
password *Header*	AppViewX login password **Type**: String **Constraints**: Required if **sessionId** is not provided.
Content-Type *Header*	Specifies the nature of the data in the payload **Type**: String
gwsource *Query*	Source from which the request is triggered. (E.g. external) **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Parameters (continued)

Name	Description
Payload *Body*	Contains all the parameters to be sent in the request body for the post request **Type**: Payload

Payload

Payload

Name	Description
generalInformation	(Mandatory) General details related to the push operation **Type**: generalInformation
certificateID	(Mandatory) Unique identifier of the certificate to be pushed
certificateDetails	(Mandatory) Details of the certificate to be pushed **Type**: certificateDetails
pushDetails	(Mandatory) Details for certificate management after the push operation **Type**: pushDetails
selectedProfiles	(Mandatory) Actual profile details of services to which where we are trying to push/bind the certificate **Type**: String

generalInformation

Name	Description
category	(Mandatory) Device type of the target system to which the certificate will be pushed **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

generalInformation (continued)

Name	Description
	Possible value(s): Cloud
vendor	(Mandatory) Cloud device vendor **Type**: String **Possible value(s)**: GCP
profileFilterSelection	(Mandatory) Service type to which the certificate will be pushed **Type**: String **Possible value(s)**: LB
name	Name given to the connector that will be created to push the certificate to the cloud device **Type**: String
profileType	(Mandatory) Type/category of the profile being used to determine how the certificate is managed after it is pushed **Type**: String **Possible value(s)**: push and bind, push only
description	Additional details related to the certificate being pushed, the connector for pushing the certificate. **Type**: String

certificateDetails

Name	Description
certificateLocation	(Mandatory) Certificate upload location **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

certificateDetails (continued)

Name	Description
	Possible value(s): • Classic Certificates (Upload your certificate and private key directly to the load balancer's configuration.) • Certificate Manager (Reference certificates managed by Certificate Manager in your load balancer configuration.)
certificateName	(Mandatory) Name of the certificate being pushed **Type**: String
isNewCertificate	(Optional) Specify if the certificate being pushed is a new certificate or an existing certificate that is being replaced **Type**: Boolean **Possible value(s)**: true, false
certificateDescription	(Optional) Additional details related to the certificate being pushed **Type**: String
profileFilterSelection	Specific profile type where the certificate will be applied **Type**: String **Possible value(s)**: LB
certificateTags	(Optional) Key-value pair attributes to add additional details about the certificate **Type**: String

pushDetails

Name	Description
scriptLocation	(Mandatory) Select the location of the script file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

pushDetails (continued)

Name	Description
	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. **Type**: String **Possible Values**: **appviewx** and **device**
preValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
postValidationScriptPath	(Mandatory if **scriptLocation** is **device**) Location of the script that will be executed before the certificate is pushed to the target system **Type**: String
pushAutomatically	Automatically push certificate to the target system, after it is renewed/reissued **Type**: Boolean **Possible value(s)**: • 1: Yes • 0: No

Response Structure

Response Structure

Name	Description
response	Contains the response attributes for the push request **Type**: response
message	Success message of the action or failure description in case of error

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response. Will be non-null for failure response. **Type**: String
tags	More info in case of failure response

Response

Name	Description
requestId	Request ID for push action for the application connector **Type**: String
connectorId	ID of the application connector for pushing the certificate **Type**: String

Status Codes

Status Codes

HTTP Status code	appStatusCode	Message and Possible Remediation
202 Accepted	**NA**	1 connector(s) saved and push operation has been triggered.
401 Unauthorized	**AVX_GW_003**	Authentication failed, reason - Invalid Credentials **Possible remediation**: Ensure that valid **username** and **password** or valid **sessionId** is provided as the header param.
400 Bad Request	**MANDATORY_FIELD_MISSING**	Mandatory field is missing or invalid - <<field name>>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes (continued)

HTTP Status code	appStatusCode	Message and Possible Remediation
		Possible remediation: Check and ensure that valid value is provided for <<field name>> field in the request.
404 Not Found	**NO_RECORDS_FOUND**	No matching records found - certificate not found. **Possible remediation**: Please provide correct value for the field **certificateId**.
400 Bad Request	**INVALID_REQUEST**	selectedProfiles are already available in the specified certificate. **Possible remediation**: Please provide a different value for the field **selectedProfiles**.
417 Expectation failed	**CERT-APP-0016**	Connector with profiles {} already exists. **Possible remediation**: Profile connector already exists for the selected certificate. Please change the **certificateId** or delete the existing connector.
500 Internal Server Error	**avx-common-011**	Error while processing

Sample Request/Response

Sample Request

```
{
  "generalInformation": {
    "category": "cloud",
    "vendor": "GCP",
    "profileFilterSelection": ":LB",
    "name": "GCP connector5",
    "description": "",
    "profileType": "Push and Bind Profiles"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 },
 "certificateDetails": {
  "certificateLocation": "Certificate Manager",
  "isNewCertificate": true,
  "certificateName": "feb10lb-cm",
  "certificateDescription": "",
  "profileFilterSelection": "Load Balancer",
  "certificateTags": {

  }
 },
 "pushDetails": {
  "scriptLocation": "appviewx",
  "preValidationScriptPath": "",
  "postValidationScriptPath": "",
  "pushAutomatically": false
 },
 "certificateId": "67a9f5ce2ff94729fda605ac",
 "selectedProfiles": [
  "GCP.Single.All:pm-project-lab-1-391708:asia-south1:test-region-internal:Application:test-region-internal-target-proxy:targetHttpsProxy:LB"
 ]
}
```


Sample Response


```
{
   "response": [
      {
         "requestId": "369",
         "connectorId":
 "GCP.Single.All:pm-project-lab-1-391708:asia-south1:test-region-internal:Application:test-region-internal-target-proxy:targetHttpsProxy:LB:@026e4051353bb9f8
8e0289d9d6ecb2e3d115b835"
      }
   ],
   "message": "1 connector(s) saved and push opertaion has been triggered.",
   "appStatusCode": null,
   "tags": {},
   "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Automation Workflows API

This guide includes comprehensive documentation on the APIs that can be used for executing different CERT+ Automation workflows.

- Enroll Certificate and Download
- Easy Certificate Provisioning
- Enroll Certificate and Push
- Enroll Certificate with ServiceNow
- Enroll Certificate and Push with ServiceNow Integration
- Renew Certificate and Push

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Renew Certificate with ServiceNow Integration
- Renew Certificate and Push With ServiceNow Integration
- Regenerate Certificate - With New CSR
- Get Request Summary/Log

Enroll Certificate and Download

This API is used to create and download certificates based on the certificate group.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Type: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
certificate_group	(Mandatory) Specifies the group to which the created certificate must be tagged. **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
ca_account	(Mandatory) CA account name of certificate authority. **Type**: String
division	(Mandatory only for DigiCert CA) Division values for DigiCert **Type**: String
cert_type	(Mandatory only for DigiCert CA) Certificate type for DigiCert and Entrust CAs **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String
digicert_entrust_organization	(Mandatory only for DigiCert CA and Entrust CA) Name of the organization **Type**: String
entrust_country	(Mandatory only for Entrust CA) Country in which the organization is located **Type**: String
entrust_additional_emails	(Mandatory only for Entrust CA) Additional email addresses
validity_unit	(Mandatory) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days
validity_value	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Integer
key_type	(Mandatory only if the input method is Manual or Policy Based) Key type of the certificate **Type**: String **Possible Values**: RSA, DSA, EC
bit_length	(Mandatory only if the input method is Manual or Policy Based) Bit length of the certificate **Type**: String **Possible Values**: 4096, 2048
hash_function	(Mandatory) Hash function for the certificate **Type**: String **Possible Values**: SHA256
elliptic_curve	(Mandatory if key type is **EC**) Elliptic curve value for the certificate **Type**: String
digicert_server_type	(Mandatory only for DigiCert CA) DigiCert server type value **Type**: String
ejbca_end_entity_user_name	(Mandatory only for EJBCA) User name of the EJBCA end entity **Type**: String
ejbca_end_entity_profile_name	(Mandatory only for EJBCA) Profile name of the EJBCA end entity **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
ejbca_issuer_common_name	(Mandatory only for EJBCA) Common name of the EJBCA issuer **Type**: String
ejbca_certificate_profile_name	(Mandatory only for EJBCA) Profile name associated with the EJBCA certificate **Type**: String
microsoft_enterprise_template_name	(Mandatory only for Microsoft Enterprise CA) Template name for Microsoft Enterprise **Type**: String
user_email	(Mandatory only for Microsoft Enterprise CA) Email address for sending status notificatiosn for certificate create and push **Type**: String
organization	(Mandatory for AppViewX CA, EJBCA, and Microsoft Enterprise CA) Name of the organization requesting the certificate **Type**: String
country	(Mandatory for AppViewx CA, EJBCA, Entrust CA, Digicert CA, and Microsoft Enterprise CA) Country in which the organization is located **Type**: String
digicert_postal_code	(Mandatory for DigiCert CA) Postal code of the organization requesting the certificate **Type**: String
description	(Optional) Certificate description

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
san	(Optional) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
dns_names	(Optional) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
ip_addresses	(Optional) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
organization_unit	(Optional) Organization unit requesting the certificate **Type**: String
locality	(Optional) Locality in which the organization is located **Type**: String
state	(Optional) State in which the organization is located **Type**: String
mail_address	(Optional) Email address of the organization **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: true, false
cert_attributes	(Mandatory if **cert_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes

Certificate Attributes

Name	Description
atrribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request

```
{
  "payload": {
    "header": {
      "workflowName": "Enroll Certificate and Download"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
},
"data": {
  "input": {
    "requestData": [
      {
        "sequenceNo": 1,
        "scenario": "scenario",
        "fieldInfo": {
          "info": "",
          "cert_category": "Server,Client,Code Signing",
          "certificate_group": "<mandatory field>",
          "certificate_authority": "DigiCert,Entrust,Ejbca,AppViewX,Microsoft Enterprise",
          "ca_account": "<mandatory field>",
          "division": "<mandatory field>",
          "cert_type": "<mandatory field>",
          "description": "",
          "common_name": "<mandatory field>",
          "san": "DNS, IP Address",
          "dns_names": "",
          "ip_addresses": "",
          "organization": "",
          "digicert_entrust_organization": "<mandatory field>",
          "organization_unit": "",
          "organization_address": "",
          "locality": "",
          "state": "",
          "country": "",
          "entrust_country": "<mandatory field>",
          "digicert_postal_code": "",
          "mail_address": "",
          "validity_unit": "Days,Months,Years",
          "validity_value": "<mandatory field>",
          "key_type": "RSA,DSA,EC",
          "bit_length": "<mandatory field>",
          "hash_function": "<mandatory field>",
          "elliptic_curve": "<mandatory field>",
          "check_attribute": "true",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "certificates_attributes": [
             {
               "attributes": "",
               "value": ""
             }
            ],
            "digicert_server_type": "<mandatory field>",
            "ejbca_end_entity_profile_name": "<mandatory field>",
            "ejbca_end_entity_user_mame": "",
            "ejbca_issuer_common_name": "<mandatory field>",
            "ejbca_certificate_profile_name": "<mandatory field>",
            "microsoft_enterprise_template_name": "<mandatory field>",
            "entrust_additional_emails": "",
            "user_email": "(~get_logged_user_email_id~)"
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "867",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Easy Certificate Provisioning

This API is used to create an AppViewX certificate and push to a device available in the instance.

Before you begin

Before attempting to trigger these service requests, ensure that:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource	(Mandatory) Source from which the request is triggered

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
Payload	Contains all the parameters to be sent in the request body for the put request.
Body	**Type**: Payload

Payload

Payload

Name	Description
appviewx_common_name	(Mandatory) Common name of the certificate. Fully qualified domain name (FQDN) of the server for which certificate is requested. **Type**: String
device_type	(Mandatory) Type of device to which the certificate will be pushed. Possible Values: ADC, Server. **Type**: String
push_devices	(Mandatory) Contains all push details. **Type**: Tabular
device_vendor	(Mandatory) Device vendor type based on selection of device type. Possible Values: F5, LinuxServer, Citrix. **Type**: String
device	(Mandatory) Device name for selected device_vendor. **Type**: String
linux_actions	(Mandatory only for the Linux server) Linux action for the selected device_vendor. Possible Values: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
selected_profiles	(Mandatory) Profile name for device. **Type**: String
apache_custom_push	(Mandatory only for the Apache server) Provision to opt for pushing the certificate to a custom location. Possible Values: Yes, No. **Type**: String
apache_certificate_location	(Mandatory only if **apache_custom_push** is set to **Yes**) Certificate path created by the user. **Type**: String
apache_key_location	(Mandatory only if **apache_custom_push** is set to **Yes**) Certificate Key path created by the user. **Type**: String
password	(Mandatory only if **linux_action** is set to **Default**) Password to access the KDB file. **Type**: String
appviewx_dns_names	(Optional) DNS values. (For example: www.appviewx.plus). Multiple values must be separated by comma (,). **Type**: String
email_id	(Optional) Email address of the organization. Possible values: Default value configured in the policy. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Easy Certificate Provisioning"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "appviewx_common_name": "<mandatory field>",
              "appviewx_dns_names": "",
              "device_type": "ADC,Server",
              "push_devices": [
                {
                  "device_vendor": "<mandatory field>",
                  "device": "<mandatory field>",
                  "linux_actions": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
                  "selected_profiles": "<mandatory field>",
                  "password": "<mandatory field>"
                }
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            ],
            "email_id": "<mandatory field>"
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```

Note: Please refer to the request structure to identify the changeable values.

Sample Response

```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "306",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 306 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
   },
   "message": "Success",
   "appStatusCode": null,
   "tags": null,
   "headers": null
}
```

References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Enroll Certificate and Push

This API is used to create a certificate and push it to the selected device.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
validity_value	(Mandatory) Validity value for the certificate **Type**: String
validity_unit	(Mandatory) Unit of validity for the certificate **Type**: String **Possible values**: Days, Months, Years
user_email	(Mandatory) Email address for sending notification of the status of certificate creation and push **Type**: String
uris	(Mandatory only for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Uniform Resource Identifier for the certificate **Type**: String
upload_csr	(Mandatory only if**input_method** is **upload_csr**) CSR for the new certificate **Type**: String
state	(Optional) State in which the organization is located **Type**: String
san	(Optional) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
rfc822names	(Mandatory only for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA)Email address(es) of the user(s) to whom the certificate is issued

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
renew_before	(Mandatory only if **auto_renew** is enabled) The renewal request will be triggered prior to the expiry date as per the selected renew_before days. **Type**: String
registered_ids	(Mandatory only for Microsoft Enterprise CA and Microsoft Standalone CA) Registered id of the certificate **Type**: String
regenerate_before	(Mandatory only if **auto_regenerate** is enabled) The regenerate request will be triggered prior to the expiry date as per the selected regenerate_before days. **Type**: String
push_devices	(Mandatory) Contains all device fields **Type**: Array of attributes
othernames	(Mandatory only for Microsoft Enterprise CA and Microsoft Standalone CA) Other names for the certificate **Type**: String
organization_unit	(Optional) Organization unit requesting the certificate **Type**: String
organization	(Mandatory only for AppViewX CA, EJBCA, and Microsoft Enterprise CA) Name of the organization requesting the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
microsoft_enterprise_template_name	(Mandatory for Microsoft Enterprise CA) Template name for Microsoft Enterprise **Type**: String
mail_address	(Optional) Email address of the organization **Type**: String
locality	(Optional) Locality in which the organization is situated **Type**: String
key_type	(Mandatory only if**input_method** is Manual or Policy Based) Key type for the certificate **Type**: String **Possible values**: RSA, DSA, EC
ip_addresses	(Optional) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
input_method	(Mandatory) Certificate creation method **Type**: String **Possible values**: Manual, Policy Based, Upload CSR
hash_function	(Mandatory) Hash function for the certificate **Type**: String **Possible Values**: SHA256

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
entrust_additional_emails	(Mandatory only for the Entrust CA) Additional email address(es) **Type**: String
elliptic_curve	(Mandatory if **key_type** = **EC**) Elliptic curve value for the certificate **Type**: String
ejbca_issuer_common_name	(Mandatory for EJBCA) Common name of the EJBCA issuer **Type**: String
ejbca_end_entity_user_name	(Mandatory for EJBCA) User name of the EJBCA end entity **Type**: String
ejbca_end_entity_profile_name	(Mandatory for EJBCA) Profile name of the EJBCA end entity **Type**: String
ejbca_certificate_profile_name	(Mandatory for EJBCA) Profile name associated with the EJBCA certificate **Type**: String
dns_names	(Optional) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
division	(Mandatory only for DigiCert CA) Division values for DigiCert **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
directory_names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Directory names for the certificate **Type**: String
digicert_server_type	(Mandatory only for DigiCert CA) DigiCert server type value **Type**: String
device_type	(Mandatory) Type of device to which the certificate will be pushed **Type**: String **Possible values**: ADC, Server
description	(Optional) Description of the certificate **Type**: String
country	(Optional) Country in which the organization is located **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: True, False **Constraints**: The **certificates_attributes** field will be passed only if **check_attribute** = **true**.
challenge_password	(Optional) Password to access the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
certificate_group	(Mandatory) Specifies the group under which the created certificate needs to be tagged **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate **Type**: String
cert_type	(Mandatory for DigiCert CA) Cert Type values for DigiCert and Entrust **Type**: String
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible values**: Server, Client
cert_attributes	Array of certificate attributes **Type**: Array of cert_attributes
ca_account	(Mandatory) CA account name of certificate authority **Type**: String
bit_length	(Mandatory only if**input_method** is Manual or Policy Based) Bit length for the certificate **Type**: String **Possible values**: 4096, 2048
auto_renew	(Mandatory) If enabled, renewal will be scheduled to trigger before expiry based on renew_before days. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
auto_regenerate	(Mandatory) If enabled, regenerate will be scheduled to trigger before expiry based on regenerate_before days. **Type**: String

cert_attributes

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Attributes for push_devices

Name	Description
device_vendor	(Mandatory) Device vendor type based on selection of device type **Type**: String **Possible values**: F5, LinuxServer, Citrix
device	(Mandatory) Device name for the selected device vendor **Type**: String
linux_actions	(Mandatory) Linux action for the selected device vendor **Type**: String **Possible values**: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb)
selected_profiles	(Mandatory) Profile name for the device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attributes for push_devices (continued)

Name	Description
	Type: String
apache_custom_new	(Mandatory for Apache devices) Provision to opt for pushing the certificate to a custom location **Type**: String **Possible values**: Yes, No
apache_certificate_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate path created by the user **Type**: String
apache_key_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate Key path created by the user **Type**: String
password	(Mandatory if **linux_actions** = **Default**) Password for accessing the KDB file **Type**: String
push_cert_type	(Mandatory) Certificate type being pushed **Type**: String

Response Structure

200 OK returns string of type application/json with the following body params:

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

Status codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status codes (continued)

HTTP Code	appStatusCode	Response Message
		Remediation: NA

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Certificate Create and Push"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "cert_category": "Server,Client,Code Signing",
              "certificate_group": "<mandatory field>",
              "certificate_authority": "DigiCert,Entrust,Ejbca,Microsoft Enterprise,Microsoft Standalone",
              "ca_account": "<mandatory field>",
              "division": "<mandatory field>",
              "cert_type": "",
              "auto_renew": "Off,On",
              "renew_before": "<mandatory field>",
              "auto_regenerate": "Off,On",
              "regenerate_before": "<mandatory field>",
              "input_method": "Manual,Policy Based,Upload CSR",
              "upload_csr": "<mandatory field>",
              "common_name": "<mandatory field>",
              "san": "DNS,IP Address",
              "directory_names": "",
              "dns_names": "",
              "rfc822names": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"ip_addresses": "",
"registered_ids": "",
"uris": "",
"othernames": "",
"organization": "",
"organization_unit": "",
"locality": "",
"state": "",
"country": "",
"mail_address": "",
"postal_code": "",
"validity_unit": "Days,Months,Years",
"validity_value": "1",
"challenge_password": "",
"hash_function": "<mandatory field>",
"key_type": "EC",
"bit_length": "<mandatory field>",
"elliptic_curve": "<mandatory field>",
"attributes_available": "true",
"cert_attributes": [
 {
   "attribute": "",
   "attribute_value": ""
 }
],
"digicert_server_type": "<mandatory field>",
"ejbca_end_entity_profile_name": "<mandatory field>",
"ejbca_end_entity_user_name": "",
"ejbca_issuer_common_name": "<mandatory field>",
"ejbca_certificate_profile_name": "<mandatory field>",
"entrust_additional_emails": "",
"microsoft_enterprise_template_name": "<mandatory field>",
"device_type": "ADC,Server",
"push_devices": [
 {
   "device_vendor": "<mandatory field>",
   "device": "<mandatory field>",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                "linux_action": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
                "selected_profiles": "<mandatory field>",
                "password": "<mandatory field>",
                "push_cert_type": "<mandatory field>"
              }
            ],
            "user_email": ""
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
    "response": {
        "workorderId": "0",
        "requestType": "default",
        "requestId": "867",
        "workflowVersion": "master",
        "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
        "status": "In Progress",
        "statusCode": 0
    },
    "message": "Success",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Enroll Certificate with ServiceNow

This API is used to create a certificate corresponding to the ticket raised on ServiceNow (RITM).

Before you begin

Before attempting to trigger these service requests, ensure that:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource	(Mandatory) Source from which the request is triggered

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
Payload	Contains all the parameters to be sent in the request body for the put request.
Body	**Type**: Payload

Payload

Payload

Name	Description
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
certificate_group	(Mandatory) Specifies the group to which the created certificate must be tagged. **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate. **Type**: String
ca_account	(Mandatory) CA account name of certificate authority. **Type**: String
division	(Mandatory only for DigiCert CA) Division values for DigiCert **Type**: String
cert_type	(Mandatory only for DigiCert CA) Certificate type for DigiCert and Entrust CAs **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
description	(Mandatory) Certificate description **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String
san	(Mandatory) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
dns_names	(Mandatory) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
ip_addresses	(Mandatory) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
organization	(Mandatory for AppViewX CA, EJBCA, and Microsoft Enterprise CA) Name of the organization requesting the certificate **Type**: String
digicert_entrust_organization	(Mandatory only for DigiCert CA and Entrust CA) Name of the organization **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
organization_unit	(Mandatory) Organization unit requesting the certificate **Type**: String
locality	(Mandatory) Locality in which the organization is located **Type**: String
state	(Mandatory) State in which the organization is located **Type**: String
country	(Mandatory for AppViewx CA, EJBCA, Entrust CA, Digicert CA, and Microsoft Enterprise CA) Country in which the organization is located **Type**: String
entrust_country	(Mandatory only for Entrust CA) Country in which the organization is located **Type**: String
digicert_postal_code	(Mandatory for DigiCert CA) Postal code of the organization requesting the certificate **Type**: String
mail_address	(Mandatory) Email address of the organization **Type**: String
validity_unit	(Mandatory) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days
validity_value	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Integer
key_type	(Mandatory only if the input method is Manual or Policy Based) Key type of the certificate **Type**: String **Possible Values**: RSA, DSA, EC
bit_length	(Mandatory only if the input method is Manual or Policy Based) Bit length of the certificate **Type**: String **Possible Values**: 4096, 2048
elliptic_curve	(Mandatory if key type is **EC**) Elliptic curve value for the certificate **Type**: String
digicert_server_type	(Mandatory only for DigiCert CA) DigiCert server type value **Type**: String
ejbca_end_entity_user_name	(Mandatory only for EJBCA) User name of the EJBCA end entity **Type**: String
ejbca_end_entity_profile_name	(Mandatory only for EJBCA) Profile name of the EJBCA end entity **Type**: String
ejbca_issuer_common_name	(Mandatory only for EJBCA) Common name of the EJBCA issuer **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
ejbca_certificate_profile_name	(Mandatory only for EJBCA) Profile name associated with the EJBCA certificate **Type**: String
entrust_additional_emails	(Mandatory only for Entrust CA) Additional email addresses
microsoft_enterprise_template_name	(Mandatory only for Microsoft Enterprise CA) Template name for Microsoft Enterprise **Type**: String
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: true, false **Constraints**: The **certificates_attributes** field will be passed only if **check_attribute** = **true**.
cert_attributes	(Mandatory if **check_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes
snow_integration	(Optional) Provision to opt for ServiceNow integration **Type**: String **Possible values**: Yes, No
snow_account	(Mandatory if **snow_integration** = **Yes**) ServiceNow account **Type**: String
download_format	(Mandatory if **snow_integration** = **Yes**) Download format for certificate tyoe **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
hash_function	(Optional) Hash function for the certificate **Type**: String **Possible Values**: SHA256
user_email	(Optional) Email address for sending status notificatiosn for certificate create and push **Type**: String

cert_attributes

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request

```
{
  "payload": {
    "header": {
      "workflowName": "Enroll Certificate with ServiceNow"
    },
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"data": {
  "input": {
    "requestData": [
      {
        "sequenceNo": 1,
        "scenario": "scenario",
        "fieldInfo": {
          "info": "",
          "cert_category": "Server,Client,Code Signing",
          "certificate_group": "<mandatory field>",
          "certificate_authority": "DigiCert,Entrust,Ejbca,AppViewX,Microsoft Enterprise",
          "ca_account": "<mandatory field>",
          "division": "<mandatory field>",
          "cert_type": "<mandatory field>",
          "description": "",
          "common_name": "<mandatory field>",
          "san": "DNS, IP Address",
          "dns_names": "",
          "ip_addresses": "",
          "organization": "",
          "digicert_entrust_organization": "<mandatory field>",
          "organization_unit": "",
          "organization_address": "",
          "locality": "",
          "state": "",
          "country": "",
          "entrust_country": "<mandatory field>",
          "digicert_postal_code": "",
          "mail_address": "",
          "validity_unit": "Days,Months,Years",
          "validity_value": "<mandatory field>",
          "key_type": "RSA,DSA,EC",
          "bit_length": "<mandatory field>",
          "hash_function": "<mandatory field>",
          "elliptic_curve": "<mandatory field>",
          "download_format": "(~get_certificate_download_format~)",
          "check_attribute": "true",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "certificates_attributes": [
             {
               "attributes": "",
               "value": ""
             }
            ],
            "digicert_server_type": "<mandatory field>",
            "ejbca_end_entity_profile_name": "<mandatory field>",
            "ejbca_end_entity_user_name": "",
            "ejbca_issuer_common_name": "<mandatory field>",
            "ejbca_certificate_profile_name": "<mandatory field>",
            "microsoft_enterprise_template_name": "<mandatory field>",
            "entrust_additional_emails": "",
            "snow_integrations": "Yes,No",
            "ritm": "<mandatory field>",
            "snow_account": "",
            "user_email": ""
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "status": "In Progress",
        "statusCode": 0
    },
    "message": "Success",
    "appStatusCode": null,
    "tags": null,
    "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enroll Certificate and Push with ServiceNow Integration

This API is used to create a certificate corresponding to the ticket raised on ServiceNow (RITM) and push it to the selected device.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
certificate_group	(Mandatory) Specifies the group to which the created certificate must be tagged. **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate. **Type**: String
ca_account	(Mandatory) CA account name of certificate authority. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
division	(Mandatory only for DigiCert CA) Division values for DigiCert **Type**: String
description	(Mandatory) Certificate description **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String
san	(Mandatory) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
dns_names	(Mandatory) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
ip_addresses	(Mandatory) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
organization	(Mandatory for AppViewX CA, EJBCA, and Microsoft Enterprise CA) Name of the organization requesting the certificate **Type**: String
digicert_entrust_organization	(Mandatory only for DigiCert CA and Entrust CA) Name of the organization

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
organization_unit	(Mandatory) Organization unit requesting the certificate **Type**: String
locality	(Mandatory) Locality in which the organization is located **Type**: String
state	(Mandatory) State in which the organization is located **Type**: String
country	(Mandatory for AppViewx CA, EJBCA, Entrust CA, Digicert CA, and Microsoft Enterprise CA) Country in which the organization is located **Type**: String
entrust_country	(Mandatory only for Entrust CA) Country in which the organization is located **Type**: String
digicert_postal_code	(Mandatory for DigiCert CA) Postal code of the organization requesting the certificate **Type**: String
mail_address	(Optional) Email address of the organization **Type**: String
validity_unit	(Optional) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
validity_value	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit **Type**: Integer
key_type	(Mandatory only if the input method is Manual or Policy Based) Key type of the certificate **Type**: String **Possible Values**: RSA, DSA, EC
bit_length	(Mandatory only if the input method is Manual or Policy Based) Bit length of the certificate **Type**: String **Possible Values**: 4096, 2048
hash_function	(Optional) Hash function for the certificate **Type**: String **Possible Values**: SHA256
elliptic_curve	(Mandatory if key type is **EC**) Elliptic curve value for the certificate **Type**: String
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: true, false **Constraints**: The **certificates_attributes** field will be passed only if **check_attribute** = **true**.
cert_attributes	(Mandatory if **check_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
snow_integration	(Optional) Provision to opt for ServiceNow integration **Type**: String **Possible values**: Yes, No
snow_account	(Mandatory if **snow_integration** = **Yes**) ServiceNow account **Type**: String
download_format	(Mandatory if **snow_integration** = **Yes**) Download format for certificate tyoe **Type**: String
device_type	(Optional) Type of device to which the certificate will be pushed **Type**: String **Possible values**: ADC, Server
push_devices	(Optional) Contains all device fields **Type**: Array of attributes

cert_attributes

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attributes for push_devices

Name	Description
device_vendor	(Mandatory) Device vendor type based on selection of device type **Type**: String **Possible values**: F5, LinuxServer, Citrix
device	(Mandatory) Device name for the selected device vendor **Type**: String
linux_actions	(Mandatory) Linux action for the selected device vendor **Type**: String **Possible values**: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb)
selected_profiles	(Mandatory) Profile name for the device **Type**: String
apache_custom_new	(Mandatory for Apache devices) Provision to opt for pushing the certificate to a custom location **Type**: String **Possible values**: Yes, No
apache_certificate_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate path created by the user **Type**: String
apache_key_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate Key path created by the user **Type**: String
password	(Mandatory if **linux_actions** = **Default**) Password for accessing the KDB file

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attributes for push_devices (continued)

Name	Description
	Type: String
push_cert_type	(Mandatory) Certificate type being pushed **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Enroll Certificate and Push with ServiceNow"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "cert_category": "Server,Client,Code Signing",
              "certificate_group": "<mandatory field>",
              "certificate_authority": "DigiCert,Entrust,Ejbca,AppViewX,Microsoft Enterprise",
              "ca_account": "<mandatory field>",
              "division": "<mandatory field>",
              "cert_type": "<mandatory field>",
              "description": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"common_name": "<mandatory field>",
"san": "DNS, IP Address",
"dns_names": "",
"ip_addresses": "",
"organization": "",
"digicert_entrust_organization": "<mandatory field>",
"organization_unit": "",
"organization_address": "",
"locality": "",
"state": "",
"country": "",
"entrust_country": "<mandatory field>",
"digicert_postal_code": "",
"mail_address": "",
"validity_unit": "Days,Months,Years",
"validity_value": "<mandatory field>",
"key_type": "RSA,DSA,EC",
"bit_length": "<mandatory field>",
"hash_function": "<mandatory field>",
"elliptic_curve": "<mandatory field>",
"download_format": "<mandatory field>",
"check_attribute": "true",
"certificates_attributes": [
 {
   "attributes": "",
   "value": ""
 }
],
"digicert_server_type": "<mandatory field>",
"ejbca_end_entity_profile_name": "<mandatory field>",
"ejbca_end_entity_user_name": "",
"ejbca_issuer_common_name": "<mandatory field>",
"ejbca_certificate_profile_name": "<mandatory field>",
"microsoft_enterprise_template_name": "<mandatory field>",
"entrust_additional_emails": "",
"device_type": "ADC,Server",
"push_devices": [
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            {
              "device_vendor": "<mandatory field>",
              "device": "<mandatory field>",
              "linux_actions": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
              "selected_profiles": "<mandatory field>",
              "password": "<mandatory field>",
              "push_cert_type": "<mandatory field>"
            }
          ],
          "snow_integrations": "Yes,No",
          "ritm": "<mandatory field>",
          "snow_account": "",
          "user_email": ""
        }
      }
    ]
  },
  "globalData": {},
  "task_action": 1
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "867",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
  "message": "Success",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Renew Certificate and Push

This API is used to renew a certificate based on the certificate group and certificate authority and push it to the selected device.

Before you begin

Before attempting to trigger these service requests, ensure that:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource	(Mandatory) Source from which the request is triggered

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
Query	**Type**: String
Payload	Contains all the parameters to be sent in the request body for the put request.
Body	**Type**: Payload

Payload

Payload

Name	Description
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
certificate_group	(Mandatory) Specifies the group to which the created certificate must be tagged. **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate. **Type**: String
serial number	(Mandatory) Serial number of the certificate **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String
san	(Mandatory) Subject Alternative Name of the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Possible values: DNS, IP Address
dns_names	(Mandatory) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
ip_addresses	(Mandatory) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
directory_names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Directory names for the certificate **Type**: String
rfc822names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Email address(es) of the user(s) to whom the certificate is issued **Type**: String
registered_ids	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Registered ID of the certificate **Type**: String
uris	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Uniform Resource Identifier of the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
othernames	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Other names for the certificate **Type**: String
validity_unit	(Mandatory) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days
validity_value	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit **Type**: Integer
digicert_server_type	(Mandatory only for DigiCert CA) DigiCert server type value **Type**: String
orderId	(Mandatory only for DigiCert CA) Order ID of the DigiCert certificate **Type**: String
ejbca_end_entity_user_name	(Mandatory only for EJBCA) User name of the EJBCA end entity **Type**: String
ejbca_end_entity_profile_name	(Mandatory only for EJBCA) Profile name of the EJBCA end entity **Type**: String
ejbca_issuer_common_name	(Mandatory only for EJBCA) Common name of the EJBCA issuer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
ejbca_certificate_profile_name	(Mandatory only for EJBCA) Profile name associated with the EJBCA certificate **Type**: String
entrust_additional_emails	(Mandatory only for Entrust CA) Additional email addresses
microsoft_enterprise_template_name	(Mandatory only for Microsoft Enterprise CA) Template name for Microsoft Enterprise **Type**: String
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: true, false **Constraints**: The **certificates_attributes** field will be passed only if **check_attribute** = **true**.
cert_attributes	(Mandatory if **check_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes
hash_function	(Optional) Hash function for the certificate **Type**: String **Possible Values**: SHA256
user_email	(Optional) Email address for sending status notificatiosn for certificate create and push **Type**: String
push_devices	(Mandatory) Contains all device fields

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: Array of attributes

cert_attributes

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Attributes for push_devices

Name	Description
device_vendor	(Mandatory) Device vendor type based on selection of device type **Type**: String **Possible values**: F5, LinuxServer, Citrix
device	(Mandatory) Device name for the selected device vendor **Type**: String
linux_actions	(Mandatory) Linux action for the selected device vendor **Type**: String **Possible values**: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb)
selected_profiles	(Mandatory) Profile name for the device **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attributes for push_devices (continued)

Name	Description
apache_custom_new	(Mandatory for Apache devices) Provision to opt for pushing the certificate to a custom location **Type**: String **Possible values**: Yes, No
apache_certificate_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate path created by the user **Type**: String
apache_key_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate Key path created by the user **Type**: String
password	(Mandatory if **linux_actions** = **Default**) Password for accessing the KDB file **Type**: String
push_cert_type	(Mandatory) Certificate type being pushed **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request

```
{
  "payload": {
    "header": {
      "workflowName": "Renew Certificate and Push"
    },
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"data": {
  "input": {
    "requestData": [
      {
        "sequenceNo": 1,
        "scenario": "scenario",
        "fieldInfo": {
          "info": "",

          "cert_category": "Server,Client",
          "certificate_group": "<mandatory field>",
          "certificate_authority": "Microsoft Enterprise,DigiCert,Ejbca,Entrust",
          "serial_number": "<mandatory field>",
          "common_name": "<mandatory field>",
          "san": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
          "dNSNames": "",
          "directoryNames": "",
          "iPAddresses": "",
          "registeredIDs": "",
          "otherNames": "",
          "uniformResourceIdentifiers": "",
          "rfc822Names": "",
          "validity_unit": "<mandatory field>",
          "validity_value": "<mandatory field>",
          "hash_function": "<mandatory field>",
          "attributes_available": "true",
          "cert_attributes": [
            {
              "attribute": "",
              "attribute_value": ""
            }
          ],
          "orderId": "",
          "digicert_server_type": "<mandatory field>",
          "ejbca_End_Entity_Profile_Name": "<mandatory field>",
          "ejbca_End_Entity_User_Name": "",
          "ejbca_Issuer_Common_Name": "<mandatory field>",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "ejbca_Certificate_Profile_Name": "<mandatory field>",
            "microsoft_enterprise_template_name": "<mandatory field>",
            "entrust_additional_emails": "",
            "push_devices": [
              {
                "device_type": "ADC,Server",
                "device_vendor": "<mandatory field>",
                "device": "<mandatory field>",
                "linux_actions": "Default,Create KDB label (*.kdb),Certificate Overwrite (*.kdb)",
                "selected_profiles": "<mandatory field>",
                "password": "<mandatory field>",
                "push_cert_type": "<mandatory field>"
              }
            ],
            "user_email": "(~get_logged_user_email_id~)"
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Renew Certificate with ServiceNow Integration

This API is used to renew a certificate based on the certificate group and certificate authority and attach the renewed certificate to the ServiceNow ticket.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
group_name	(Mandatory) Specifies the group to which the created certificate must be tagged. **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate. **Type**: String
ca_account	(Mandatory) Account name of the selected CA
serial number	(Mandatory) Serial number of the certificate **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
san_type	(Mandatory) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
dNSNames	(Mandatory) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
iPAddresses	(Mandatory) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
directory_names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Directory names for the certificate **Type**: String
uniformResourceIdentifiers	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Uniform Resource Identifier for the certificate **Type**: String
registered_ids	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Registered ID of the certificate **Type**: String
othernames	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Other names for the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
validity	(Mandatory) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days
validity_value	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit **Type**: Integer
hash_function	(Optional) Hash function for the certificate **Type**: String **Possible Values**: SHA256
cert_attributes	(Mandatory if **check_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes
hash_function	(Optional) Hash function for the certificate **Type**: String **Possible Values**: SHA256
user_email	(Optional) Email address for sending status notificatiosn for certificate create and push **Type**: String
email_ID	(Optional) Email address of the organization requesting the certificate **Type**: String
snow_integration	(Optional) Provision to opt for ServiceNow integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Possible values**: Yes, No
ritm	(Mandatory if **snow_integration** = **Yes**) RITM ticket number of the ServiceNow ticket **Type**: String
snow_account	(Mandatory if **snow_integration** = **Yes**) ServiceNow account **Type**: String
download_format	(Mandatory if **snow_integration** = **Yes**) Download format for certificate tyoe **Type**: String
show_validity	(Optional) Hidden field inside the form. **Type**: String

Attribute details

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Attributes for push_devices

Name	Description
device_vendor	(Mandatory) Device vendor type based on selection of device type

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attributes for push_devices (continued)

Name	Description
	Type: String **Possible values**: F5, LinuxServer, Citrix
device	(Mandatory) Device name for the selected device vendor **Type**: String
linux_actions	(Mandatory) Linux action for the selected device vendor **Type**: String **Possible values**: Default, Create KDB label (*.kdb), Certificate Overwrite (*.kdb)
selected_profiles	(Mandatory) Profile name for the device **Type**: String
apache_custom_new	(Mandatory for Apache devices) Provision to opt for pushing the certificate to a custom location **Type**: String **Possible values**: Yes, No
apache_certificate_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate path created by the user **Type**: String
apache_key_location	(Mandatory if **apache_custom_new** = **Yes**) Certificate Key path created by the user **Type**: String
password	(Mandatory if **linux_actions** = **Default**) Password for accessing the KDB file **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attributes for push_devices (continued)

Name	Description
push_cert_type	(Mandatory) Certificate type being pushed **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Renew Certificate"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
            "fieldInfo": {
              "info": "",
              "category": "Server,Client",
              "group_name": "<mandatory field>",
              "policy_hidden": "",
              "certificate_authority": "<%certificate_authority%>",
              "certificate": "",
              "ca_account": "",
              "comman_name": "<mandatory field>",
              "san_type": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
              "dNSNames": "",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"iPAddresses": "",
"rfc": "",
"directory_names": "",
"uniformResourceIdentifiers": "",
"otherNames": "",
"registeredIDs": "",
"division": "",
"organisation": "",
"organisation_unit": "",
"country": "",
"city": "",
"state": "",
"postalcode": "",
"mailaddress": "",
"validity": "",
"validity_value": "",
"hash_function": "<mandatory field>",
"bit_length": "",
"key_type": "",
"attrib_details": [
 {
   "cert_attribute_name": "",
   "cert_attribute_value": ""
 }
],
"order_id": "",
"server_type": "",
"order_validity": "",
"order_val_till": "",
"end_entity_profile_name": "",
"end_entity_user_name": "",
"issuer_common_name": "",
"certificate_profile_name": "",
"template_name": "",
"additional_email": "",
"resource": "",
"serial_number": "<mandatory field>",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "email_id": "(~get_logged_user_email_id~)",
            "ca": "",
            "description": ""
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
   },
   "message": "Success",
   "appStatusCode": null,
   "tags": null,
   "headers": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Renew Certificate and Push With ServiceNow Integration

This API is used to renew a certificate based on the certificate group and certificate authority, push it to a device, and attach the renewed certificate to the ServiceNow ticket.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload

Payload

Name	Description
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
certificate_group	(Mandatory) Specifies the group to which the created certificate must be tagged. **Type**: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate. **Type**: String
serial number	(Mandatory) Serial number of the certificate **Type**: String
common_name	(Mandatory) Common name of the certificate **Type**: String
san	(Mandatory) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
dns_names	(Mandatory) DNS values **Type**: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
ip_addresses	(Mandatory) IP values

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
directory_names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Directory names for the certificate **Type**: String
rfc822names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Email address(es) of the user(s) to whom the certificate is issued **Type**: String
uris	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Uniform Resource Identifier for the certificate **Type**: String
registered_ids	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Registered ID of the certificate **Type**: String
othernames	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Other names for the certificate **Type**: String
validity_unit	(Mandatory) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
validity_value	(Mandatory if validityUnit has been specified) Number of units of the time specified as the validity unit **Type**: Integer
hash_function	(Mandatory) Hash function for the certificate **Type**: String **Possible Values**: SHA256
digicert_server_type	(Mandatory only for DigiCert CA) DigiCert server type value **Type**: String
orderId	(Mandatory only for DigiCert CA) Order ID of the DigiCert certificate **Type**: String
ejbca_end_entity_user_name	(Mandatory only for EJBCA) User name of the EJBCA end entity **Type**: String
ejbca_end_entity_profile_name	(Mandatory only for EJBCA) Profile name of the EJBCA end entity **Type**: String
ejbca_issuer_common_name	(Mandatory only for EJBCA) Common name of the EJBCA issuer **Type**: String
ejbca_certificate_profile_name	(Mandatory only for EJBCA) Profile name associated with the EJBCA certificate **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
entrust_additional_emails	(Mandatory only for Entrust CA) Additional email addresses
microsoft_enterprise_template_name	(Mandatory only for Microsoft Enterprise CA) Template name for Microsoft Enterprise **Type**: String
user_email	(Optional) Email address for sending status notificatiosn for certificate create and push **Type**: String
snow_integration	(Optional) Provision to opt for ServiceNow integration **Type**: String **Possible values**: Yes, No
ritm	(Mandatory if **snow_integration** = **Yes**) RITM ticket number of the ServiceNow ticket **Type**: String
snow_account	(Mandatory if **snow_integration** = **Yes**) ServiceNow account **Type**: String
download_format	(Mandatory if **snow_integration** = **Yes**) Download format for certificate tyoe **Type**: String
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: true, false **Constraints**: The **certificates_attributes** field will be passed only if **check_attribute** = **true**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
cert_attributes	(Mandatory if **check_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes

Attribute details

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request


```
{
  "payload": {
    "header": {
      "workflowName": "Renew Certificate and Push with ServiceNow"
    },
    "data": {
      "input": {
        "requestData": [
          {
            "sequenceNo": 1,
            "scenario": "scenario",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "fieldInfo": {
          "info": "",
          "cert_category": "Server,Client",
          "certificate_group": "<mandatory field>",
          "certificate_authority": "<mandatory field>",
          "serial_number": "<mandatory field>",
          "common_name": "<mandatory field>",
          "san": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
          "dNSNames": "",
          "directoryNames": "",
          "iPAddresses": "",
          "registeredIDs": "",
          "otherNames": "",
          "uniformResourceIdentifiers": "",
          "rfc822Names": "",
          "validity_unit": "<mandatory field>",
          "validity_value": "<mandatory field>",
          "hash_function": "",
          "download_format": "(~get_certificate_download_format~)",
          "cert_attributes": [
            {
              "attributes": "",
              "attribute_value": ""
            }
          ],
          "snow_integrations": "Yes,No",
          "ritm": "<mandatory field>",
          "snow_account": "(~get_ServiceNow_accounts~)",
          "user_email": "(~get_logged_user_email_id~)"
        }
      }
    ]
  },
  "globalData": {},
  "task_action": 1
}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
 }
}
```

Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workorderId": "0",
      "requestType": "default",
      "requestId": "867",
      "workflowVersion": "master",
      "message": "Workflow Request is created with Id 867 . Request submitted to workflow engine for processing workorder.",
      "status": "In Progress",
      "statusCode": 0
   },
   "message": "Success",
   "appStatusCode": null,
   "tags": null,
   "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Regenerate Certificate - With New CSR

This API is used to regenerate a certificate with a new CSR.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-submit-request
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-submit-request?gwsource=external` To understand the elements of the sample URL, click here.
Headers	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the put request. **Type**: Payload

Payload

Payload

Name	Description
cert_category	(Mandatory) Specifies the certificate category **Type**: String **Possible Values**: Server, Client
certificate_group	(Mandatory) Specifies the group to which the created certificate must be tagged.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
certificate_authority	(Mandatory) Name of the certificate authority that will issue the certificate. **Type**: String
ca_account	CA account name of the certificate Authority **Type**: String
division	(Mandatory only for DigiCert CA) Division values for DigiCert **Type**: String
cert_type	(Mandatory only for DigiCert CA) Certificate type for DigiCert and Entrust CAs **Type**: String
input_method	(Mandatory) Certificate creation method **Type**: String **Possible values**: Manual, Policy Based, Upload CSR
upload_csr	(Mandatory if **input_method** = **Upload CSR**) CSR for the new certificate
common_name	(Mandatory) Common name of the certificate **Type**: String
san	(Mandatory) Subject Alternative Name of the certificate **Type**: String **Possible values**: DNS, IP Address
dns_names	(Mandatory) DNS values

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String **Example**: www.appviewx.com **Constraints**: Multiple values must be separated by a comma (,).
ip_addresses	(Mandatory) IP values **Type**: String **Example**: 192.16x.xx.x **Constraints**: Multiple values must be separated by a comma (,).
directory_names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Directory names for the certificate **Type**: String
rfc822names	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Email address(es) of the user(s) to whom the certificate is issued **Type**: String
uris	(Mandatory for EJBCA, Microsoft Enterprise CA, and Microsoft Standalone CA) Uniform Resource Identifier for the certificate **Type**: String
registered_ids	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Registered ID of the certificate **Type**: String
othernames	(Mandatory for Microsoft Enterprise CA and Microsoft Standalone CA) Other names for the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
organization	(Mandatory for AppViewX CA, EJBCA, and Microsoft Enterprise CA) Name of the organization requesting the certificate **Type**: String
organization_unit	(Mandatory) Organization unit requesting the certificate **Type**: String
locality	(Mandatory) Locality in which the organization is located **Type**: String
state	(Optional) State in which the organization is located **Type**: String
country	(Mandatory for AppViewx CA, EJBCA, Entrust CA, Digicert CA, and Microsoft Enterprise CA) Country in which the organization is located **Type**: String
mail_address	(Mandatory) Email address of the organization **Type**: String
challenge_password	(Optional) Password to access the certificate **Type**: String
validity_unit	(Optional) Unit of time for the certificate's validity period **Type**: String **Possible values**: years, months, days

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
validity_value	(Mandatory if **validityUnit** has been specified) Number of units of the time specified as the validity unit **Type**: Integer
key_type	(Mandatory only if the input method is Manual or Policy Based) Key type of the certificate **Type**: String **Possible Values**: RSA, DSA, EC
bit_length	(Mandatory only if the input method is Manual or Policy Based) Bit length of the certificate **Type**: String **Possible Values**: 4096, 2048
hash_function	(Optional) Hash function for the certificate **Type**: String **Possible Values**: SHA256
digicert_server_type	(Mandatory only for DigiCert CA) DigiCert server type value **Type**: String
ejbca_end_entity_user_name	(Mandatory only for EJBCA) User name of the EJBCA end entity **Type**: String
ejbca_end_entity_profile_name	(Mandatory only for EJBCA) Profile name of the EJBCA end entity **Type**: String
ejbca_issuer_common_name	(Mandatory only for EJBCA) Common name of the EJBCA issuer

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Type: String
ejbca_certificate_profile_name	(Mandatory only for EJBCA) Profile name associated with the EJBCA certificate **Type**: String
entrust_additional_emails	(Mandatory only for Entrust CA) Additional email addresses
microsoft_enterprise_template_name	(Mandatory only for Microsoft Enterprise CA) Template name for Microsoft Enterprise **Type**: String
user_email	(Optional) Email address for sending status notificatiosn for certificate create and push **Type**: String
check_attribute	(Optional) Certificate attribute values **Type**: String **Possible values**: true, false **Constraints**: The **certificates_attributes** field will be passed only if **check_attribute** = **true**.
cert_attributes	(Mandatory if **check_attributes** = **true**) Certificate attribute settings **Type**: Array of certificate attributes

Attribute details

Name	Description
attribute	(Optional) Certificate attribute name **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Attribute details (continued)

Name	Description
attribute_value	(Optional) Corresponding certificate attribute value **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Response
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response **Type**: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response (continued)

Name	Description
	Type: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success **Remediation**: NA
400 Bad Request	avx-common-028	Invalid/ Incorrect payload **Remediation**: Check and ensure if a valid value is given in the request payload field - input.
401 Unauthorized	WORKFLOW_1679	User is not authorized. **Remediation**: Ensure that logged-in user is authorized to access the workflow.
404 Not Found	engine-db-015	Workflow not found. **Remediation**: Ensure the workflow data is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
409 Conflict	WORKFLOW_1475	Given workflow is not in enabled state. **Remediation**: Enable the workflow.
500 Internal Server Error	WORKFLOW_1617	Invalid form data. Please provide all mandatory data **Remediation**: Ensure a valid value is given in the request payload field - input.
500 Internal Server Error	NA	Error while processing **Remediation**: NA

Sample Request/Response

Sample Request


```
{
 {
 "payload": {
  "header": {
   "workflowName": "Regenerate Certificate - With New CSR"
  },
  "data": {
   "input": {
    "requestData": [
     {
      "sequenceNo": 1,
      "scenario": "scenario",
      "fieldInfo": {
       "info": "",
       "cert_category": "Server,Client",
       "certificate_group": "<mandatory field>",
       "certificate_authority": "Ejbca,Microsoft Enterprise,DigiCert,Entrust",
       "ca_account": "<mandatory field>",
       "division": "",
       "cert_type": "",
       "serial_number": "<mandatory field>",
       "input_method": "Manual,Upload CSR",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"cert_profile": "",
"upload_csr": "<mandatory field>",
"fetch_csr_params": "",
"common_name": "<mandatory field>",
"csr_common_name": "",
"san": "DNS,Directory Name,Email,IP Address,Registered ID,URL,Other Name",
"csr_san": "DNS,Directory Name,IP Address,Registered ,ID,URL,Other Name,Email",
"csr_dns": "",
"dNSNames": "",
"directoryNames": "",
"iPAddresses": "",
"registeredIDs": "",
"otherNames": "",
"uniformResourceIdentifiers": "",
"rfc822names": "",
"organization": "",
"csr_iPAddresses": "",
"csr_uniformResourceIdentifiers": "",
"csr_directoryNames": "",
"csr_registeredIDs": "",
"csr_otherNames": "",
"csr_rfc822names": "",
"csr_organization": "",
"organization_unit": "",
"csr_organization_unit": "",
"locality": "",
"csr_locality": "",
"state": "",
"csr_state": "",
"country": "",
"csr_email_address": "",
"mail_address": "",
"challenge_password": "",
"csr_challenge_password": "",
"csr_country": "",
"digicert_postal_code": "",
"validity_unit": "<mandatory field>",
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "validity_value": "<mandatory field>",
            "csr_key_type": "EC",
            "key_type": "EC",
            "bit_length": "<mandatory field>",
            "csr_bit_length": "",
            "hash_function": "<mandatory field>",
            "csr_hash_function": "",
            "attributes_available": "true",
            "cert_attributes": [
             {
               "attributes": "",
               "attribute_value": ""
             }
            ],
            "ejbca_End_Entity_Profile_Name": "<mandatory field>",
            "ejbca_End_Entity_User_Name": "",
            "ejbca_Issuer_Common_Name": "<mandatory field>",
            "ejbca_Certificate_Profile_Name": "<mandatory field>",
            "digicert_server_type": "<mandatory field>",
            "microsoft_enterprise_template_name": "<mandatory field>",
            "entrust_additional_emails": "",
            "user_email": "(~get_logged_user_email_id~)"
          }
        }
      ]
    },
    "globalData": {},
    "task_action": 1
  }
 }
}
```


Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
  {
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "response": {
    "workorderId": "0",
    "requestType": "default",
    "requestId": "867",
    "workflowVersion": "master",
    "message": "Workflow Request is created with Id 897 . Request submitted to workflow engine for processing workorder.",
    "status": "In Progress",
    "statusCode": 0
  },
  "message": "Success",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


References

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Get Request Summary/Log

After you are done submitting a workflow you can get the request summary/logs details of a particular workflow request. The execution details of the workflow can be viewed from these logs.

Before you begin

Before attempting to trigger these service requests, ensure that:

- The workflow is enabled.

> **Note:** For more information on how to enable a workflow, refer the section on Managing Certificates using Automation Workflows.

- The API user has the necessary RBAC permissions to trigger the workflow. You can check this in the **Platform** module under **IDENTITY** > **Role** > **Authorized functions**.

Request Structure

Endpoint:	/visualworkflow-request-logs
Type:	GET
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/visualworkflow-request-logs?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Input Parameters

Name	Description
sessionId *Header*	(Mandatory, if **username** and **password** are not provided) Session ID received after login. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
username *Header*	(Mandatory if **sessionId** is not provided) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory if **sessionId** is not provided) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
gwsource *Query*	(Mandatory) Source from which the request is triggered **Type**: String
ids *Query*	Request ID **Type**: String

Response Structure

Response Structure

Name	Description
response	Contains the response params for the search object request. **Type**: Key-value pair
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response Will be non-null for failure response **Type**: String
tags	More information in case of a failure response

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Response Structure (continued)

Name	Description
	Type: NA

Response

Name	Description
requestId	Unique identifier for the request **Type**: String
workflowVersion	Version of the workflow **Type**: String
message	The message with the status and request number for the request **Type**: String
status	Status of the request **Type**: String
stausCode	Status code for the request **Type**: String
requestType	Request type **Type**: String
workorderId	The ID of the work order for the request If there is no workorder, the value will be 0. **Type**: String

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Success

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

HTTP Code	appStatusCode	Response Message
		Remediation: NA
400 Bad Request	WORKFLOW_1300	Workflow request ID is mandatory. **Remediation**: Ensure that a valid workflow request ID is provided in the request.
404 Not Found	engine-db-011	Request not found. Invalid workflow data. **Remediation**: Ensure the workflow data is valid.

Sample Request/Response

Sample Request

NA

Note: Please refer to the request structure to identify the changeable values.

Sample Response


```
{
   "response": {
      "workOrderList": [
         {
            "statusCode": 1,
            "requestId": "410",
             "created_by": "admin",
            "status": "Completed",
            "workflowName": "Copy of reviewComponent Test",
             "toolTip": null,
            "workorder_id": null,
             "description": null,
            "ticket_details": null,
            "tasks": [
               {
                  "state": 1,
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                    “comments”:null,
                    "task_name": "WorkOrder",
                    "task_id": "startWorkOrder_1",
                    "user": "admin",
                    "task_status": "Success",
                    "task_start_time": 1502696313667,
                    "task_end_time": 1502696729781,

                    "logs": [
                        {
                            "time": 1502696313815,
                            "message": "Child WorkOrder ID: 1, has been created for the Child workflow: WorkOrder"
                        },
                        {
                            "time": 1502696729781,
                            "message": "WorkOrder Completed"
                        }
                    ]
                }
            ],
            "created_time": 1502696305239,
            "rollback_reference_id": "",
            "clone_reference_ids": [],
            "last_updated": 1502696305239,
            "runnning_time": 0
        }
    ]
  },
  "message": null,
  "appStatusCode": null,
  "tags": null
}
```


References

Understanding the sample URL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

After you are done

- Once an action has been triggered, a request will be created for that.
- Requests have to be approved using the Approve request action.
- Requests have to be approved using the Implement request action.
- Approve a Request
- Implement a Request

Approve a Request

The approve a request API approves the certificate request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Request Structure

Endpoint:	/certificate/workorder/update
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/workorder/update?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.
  - **HostName**: A human-readable label assigned to a device (host) on a network

    The hostname will be included in the endpoint URL for an on-prem deployment.
  - **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

    The tenant name will be included in the endpoint URL for a SaaS deployment.
- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**
- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters

Name	Description
sessionId *Header*	(Mandatory) Session Id received after login. **Type**: String **Constraint**: Required if username and password are not provided.
username *Header*	(Mandatory) AppViewX login username. **Type**: String **Constraint**: Required if sessionId is not provided.
password *Header*	(Mandatory) AppViewX login password. **Type**: String **Constraint**: Required if sessionId is not provided.
Content-Type *Header*	(Mandatory) Specifies the nature of the data in the payload. **Type**: String **Constraint**: Value of the parameter should be **'application/json'**.
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the POST request. **Type**: Payload

Payload

Name	Description
data	(Mandatory) Contains the action data. **Type**: String
task_action	(Mandatory) Action to be performed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
data	**Type**: Number **Constraint**: Values are **1** for approve and **2** for reject.
header	(Mandatory) Contains the request details. **Type**: String
request_id	Id of the request. header **Type**: String
workorder_id	Id of the workorder. header **Type**: String **Constraint**: Value should be **0**.
task_id	Id of the task to be performed. header **Type**: String **Constraint**: Value should be **review_1**.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the approve request.
requestId	Request id for approve action for the application connector. response **Type**: String
message	Success message of the action or a failure description in case of an error. response **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Parameters (continued)

Name	Description
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Request submitted to workflow engine for processing workflow request 14.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
404 Not Found	engine-db-011	Request not found. **Remediation**: Ensure that a valid value is provided for the request_id field in the request.

Sample Request/Response

Request Payload

```
{
 "data": {
 "task_action": 1
 },
 "header": {
 "request_id": "14",
 "workorder_id": "0",
 "task_id": "review_1"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
}
}
```

Response

```
{
"response": {
"message": "Request submitted to workflow engine for processing workflow request 14",
"requestId": "14"
},
"message": "Success",
"appStatusCode": null,
"tags": {},
"headers": null
}
```

Implement a Request

The implement request API implements the request for the certificate.

Request Structure

Endpoint:	/certificate/workorder/update
Type:	POST
Sample URL:	`https://<IP/HostName/TenantName>:<GWPORT>/avxapi/certificate/workorder/update?gwsource=external` To understand the elements of the sample URL, click here.
Headers	
Content-Type:	application/json

Understanding the sample URL

- **IP/HostName/TenantName**: Replace with the actual IP address, hostname, or tenant name based on the specific configuration in AppViewX.
  - **IP**: A unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication

    The IP address will be included in the endpoint URL for an on-prem deployment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **HostName**: A human-readable label assigned to a device (host) on a network

  The hostname will be included in the endpoint URL for an on-prem deployment.

- **TenantName**: An identifier label for a tenant given to indicate which tenant's data the API request will access/modify

  The tenant name will be included in the endpoint URL for a SaaS deployment.

- **GWPORT**: AppViewX gateway port

  A gateway port refers to a network port through which data is sent and received to communicate with a gateway in an on-prem deployment.

  Example: **31443**

- **avxapi**: Path parameter value (static) that is part of the endpoint's URL
- **Endpoint**: Endpoint of the API, for example: **execute-hook**
- **gwsource**: Source or origin of a gateway, for example: **external**.

Input Parameters

Name	Description
sessionId	(Mandatory) Session Id received after login.
Header	**Type**: String
	Constraint: Required if username and password are not provided.
username	(Mandatory) AppViewX login username.
Header	**Type**: String
	Constraint: Required if sessionId is not provided.
password	(Mandatory) AppViewX login password.
Header	**Type**: String
	Constraint: Required if sessionId is not provided.
Content-Type	(Mandatory) Specifies the nature of the data in the payload.
Header	**Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Input Parameters (continued)

Name	Description
	Constraint: Value of the parameter should be **'application/json'**
gwkey *Query*	(Mandatory) Tenant Key. This is needed only in case of multi-tenant installations and can disregarded for other types of installations. **Type**: String
gwsource *Query*	(Mandatory) Source from which the request is triggered. (E.g. external) **Type**: String
Payload *Body*	Contains all the parameters to be sent in the request body for the POST request. **Type**: Payload

Payload

Name	Description
data	(Mandatory) Contains the action data. **Type**: String
task_action data	(Mandatory) Action to be performed. **Type**: Number **Constraint**: Values are **1** for approve and **2** for reject.
header	(Mandatory) Contains the request details. **Type**: String
request_id header	Id of the request. **Type**: String
workorder_id header	Id of the workorder. **Type**: String

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Payload (continued)

Name	Description
	Constraint: Value should be **0**.
task_id `header`	Id of the task to be performed. **Type**: String **Constraint**: Value should be **review_1**.

Response Structure

Response returns string of type application/json with the following body parameters:

Parameters

Name	Description
response	Contains the response attributes for the implement request.
requestId `response`	Request id for implement action for the application connector. **Type**: String
message `response`	Success message of the action or a failure description in case of an error. **Type**: String
message	Success message or failure description in case of error. **Type**: String
appStatusCode	Application specific status code for the response. It is a non-null value for a failure response. **Type**: String
tags	Additional information in case of failure response.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Status Codes

HTTP Code	appStatusCode	Response Message
200 OK	NA	Request submitted to workflow engine for processing workflow request 14.
401 Unauthorized	AVX_GW_003	Authentication failed, reason - Invalid Credentials. **Remediation**: Ensure that valid username and password or valid sessionId is provided as header parameters.
404 Not Found	engine-db-011	Request not found. **Remediation**: Ensure that a valid value is provided for the request_id field in the request.

Sample Request/Response

Request Payload


```
{
 "data": {
 "task_action": 1
 },
 "header": {
 "request_id": "14",
 "workorder_id": "0",
 "task_id": "review_2"
 }
 }
```


Response


```
{
"response": {
 "message": "Request submitted to workflow engine for processing workflow request 14",
 "requestId": "14"
 },
 "message": "Success",
 "appStatusCode": null,
 "tags": {},
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
"headers": null

}
```


Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 5: CERT+ Troubleshooting Guide

This guide helps you troubleshoot some common problems that can occur while executing CLM actions.

- Troubleshooting for CAs
- Troubleshooting General
- Troubleshooting Auto-Enrolment Protocols
- Troubleshooting AWS, CLOUD
- Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

Troubleshooting for CAs

- Troubleshooting for Amazon CA Issues
- Troubleshooting for Custom CA Issues
- Troubleshooting for DigiCert CA Issues
- Troubleshooting for EJBCA CA Issues
- Troubleshooting for Entrust MPKI Issues
- Troubleshooting for GlobalSign CA Issues
- Troubleshooting for GoDaddy CA Issues
- Troubleshooting for Google Private CA Issues
- Troubleshooting for InCommon CA Issues
- Troubleshooting for LetsEncrypt CA Issues
- Troubleshooting for Microsoft Enterprise CA Issues
- Troubleshooting for Microsoft Standalone CA Issues
- Troubleshooting Sectigo CA
- Troubleshooting Symantec CA
- Troubleshooting Trustwave CA
- Troubleshooting the Windows Agent Setup

Troubleshooting for Amazon CA Issues

This section will guide you in troubleshooting the common problems that you might encounter when using Amazon CA functionalities like setting addition, enrollment, renewal, regeneration, and revocation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Configuring Amazon CA

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Amazon already exists in inventory.	Check the CA setting name; it should be unique.
Please provide information as required.	Some of the mandatory fields might be missing or might be invalid.	Add valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Connection failed due to incorrect CA settings details : The request signature we calculated does not match the signature you provided. Check your AWS Secret Access Key and signing method.	Secret access key or access key is incorrect.	Please check the provided access key and secret key is valid.
Unable to establish connection with CA.	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling an Amazon CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Error while requesting certificate	• Domain validation failed in amazon CA. • Exceeded the limit for new certificates.	• Validate the provided domain is as per standard. • Check whether certificate enrollment has reached the limit in amazon.
Error while fetching cert	Enrollment requests may be in progress on the Amazon side.	Retry the action after some time.
Unable to establish connection with CA	• The configured CA details may be incorrect. • Proxy details may not be configured. • AppViewX may not be able to reach CA.	• Check the CA details configured on the CA settings page. • Check whether proxy details are configured in proxy settings. Check whether network access is available.
Unable to establish connection, Please ensure Proxy / Internet connectivity.	• Internet connectivity may be unavailable. • Invalid URL provided in CA Settings.	• Please check Internet connectivity to reach CA. • Please Check whether a valid CA URL is provided in CA Settings or Contact Support Team.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or contact AppViewX Support

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Too many create certificate requests	Too many create certificate requests for Amazon.	Please try to create a certificate request after some time or contact AppViewX Support

Issues in Renewing an Amazon Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Look for an email from ACM, and then follow the link in that email to validate your domain	Domain validation required	Check for email triggered from ACM to validate the domain.
One or more domain names were not validated before the certificate expired, and ACM did not renew the certificate. You can request a new certificate.	Issue in domain name validation.	Check whether the provided domain is valid.
ACM hasn't started the managed renewal process for this certificate.	ACM has not started the renewal request for the provided certificate.	Retry the request after some time.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support
Too many create certificate requests	Too many create certificate requests for Amazon.	Please try to create a certificate request after some time or contact AppViewX Support

Issues in Regenerating an Amazon CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Error while requesting certificate	Domain validation failed in amazon CA.	Validate the provided domain is as per standard.
	Exceeded limit for a new certificate.	Check whether certificate enrollment has reached the limit in amazon.
Error while fetching cert	Enrollment requests may be in progress on the Amazon site.	Retry the action after some time.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in the Amazon server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or contact AppViewX Support

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Too many create certificate requests	Too many create certificate requests for Amazon	Please try to create a certificate request after some time or contact AppViewX Support

Issues in Revoking an Amazon CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
AWS Premium Support Subscription is required to use this service. This certificate can be revoked by submitting a ticket with AWS support.	Amazon does not support certificate revoke.	Check with Amazon premium support for getting revoke service.

Troubleshooting for Custom CA Issues

This section will help you troubleshoot the common problems that you might encounter when using Custom CA functionalities like setting addition, enrollment, fetching, renewal, regeneration, and revocation.

Supported Web Browsers

Error messages and resolutions

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Devices

Error messages and resolutions

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Configuring Custom CA and Custom CA Fetch CA Names

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Failed to add custom CA details as name already exists	A CA setting with the same name for Custom CA already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty.** • **Mandatory Field(s) - <Field name> is/are empty.** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Upload a valid CA certificate in .pfx format	Upload certificate not in .pfx or .p12 format	Upload the certificate in either of pfx or p12 format
Uploaded CA certificate already exist	Uploaded certificate already exists.	Uploaded a new certificate
Issuer serial number is mandatory on request.	Issuer serial number is missing.	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing.	Please provide ca certificate details

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling a Custom CA certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide ca certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the field
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Fetching a Custom CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Entered order id is invalid.	Order ID is invalid.	Provide valid order ID.

Issues in Renewing a Custom CA certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide CA certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Regenerating a Custom CA certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid issuer details are specified in the request.	Issuer details are missing	Please provide issuer details
Issuer serial number is mandatory on request.	Issuer serial number is missing	Please provide issuer serial number
CA certificate details are missing	CA certificate details are missing	Please provide ca certificate details
Field cannot be empty.	Mandatory field is missing	Please provide the values for the field
Invalid CSR.	Specified CSR is invalid	Provide a valid CSR

Issues in Revoking a Custom CA certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Serial number or revocation request is null or empty.	Invalid request or invalid serial number specified.	Provide the valid request.
The certificate cannot be revoked as it does not have CRL distribution point.	Certificate does not have a CRL distribution point.	Invalid serial number provided.
The certificate is already revoked.	Certificate is already revoked.	Already revoked, so I need to revoke again.
Entered revocation reason is invalid.	Invalid reason specified	Specify valid reason to revoke the certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting for DigiCert CA Issues

This section helps you troubleshoot the common problems that you might encounter when using Digicert CA functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Configuring DigiCert CA

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Digicert already exists in inventory.	Check the CA Setting name, it should be unique.
Fetch certificate types action has failed Connection failed due to incorrect CA settings details	Please check the Service URL or API Access key.	Verify the service URL configured: Sample URL: https://www.digicert.com/services/v2/.
Fetch certificate types action has failed Access denied due to missing permission.	Access Key may be wrong or may not have enough authorization.	Verify the Access key and check its API authorization, it should be set as none.
Fetch certificate types action has failed Proxy details is not configured in proxy settings	Proxy details might have not been configured.	Configure valid proxy details.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling a DigiCert Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Renewing a DigiCert Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide a valid order Id of the certificate.	OrderId may be incorrect to perform CLM action in Digicert	Verify the orderid of the certificate from the Digicert CA account.
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating a DigiCert CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Revoking a DigiCert certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Error while revoking certificate-The specified order was not found.	The order id provided in the connector might be wrong.	Check the orderId for the certificate in Digicert CA Portal.
Error while revoking certificate-Order Id not provided to get corresponding certificate Id.	orderid is not provided for the action	Provide a valid order id to proceed with the action.
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Discovering DigiCert CA Certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Service unavailable, please limit request volume	DigiCert throws a service unavailable error, please limit request volume when: • 1000+ continuous requests fired, So with buffer to enroll certificates, 900 certificate requests • only be fired in a batch	AppViewX CERT+ discovery automatically handles it by introducing a delay of 50 minutes between each 900 requests.

Troubleshooting for EJBCA CA Issues

This section helps you troubleshoot the common problems that you might encounter when using EJBCA CA functionalities like EJBCA CA setting addition, certificate enrollment, renewal, revocation, suspension, reinstatement, and discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Configuring EJBCA CA and Fetching EEPs

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for EJBCA already exists in the inventory.	Check the CA Setting name. It should be unique.
• **This field should not be null or empty.** • **Mandatory Field(s) - <Field name> is/are empty.** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please enter valid credentials - Certificate and key, URL	Uploaded client certificate is incorrect or does not have the required permissions.	Please check the uploaded certificate and its permissions. Ensure that the required permissions are assigned.
At least one end entity profile should be added.	CA Setting does not have at least one End entity profile selected and added.	CA Settings should have at least one End entity profile selected and added.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Issues in Enrolling an EJBCA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Subject DN field <FieldName>must exist.	FieldName may be set as mandatory in the selected End entity profile in EJBCA portal.	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (If the field is Organization, Organization unit, Locality, Country, State). If the field is not listed on the enrollment page, add the field in the End entity profile, then pass the value via the enrollment page.
Unable to submit the CSR request to certificate authority - Wrong number of <FieldName> fields in Subject Alternative Name.	No. of values sent and no. of values configured for the field do not match.	1. Send the exact no of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal to match the sending value count.
Unable to submit the CSR request to certificate authority - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles.	Certificate profiles may not be configured in the selected end entity profile.	Configure the selected certificate profile in the selected end entity profile.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/ EJBCA server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in EJBCA server for creating certificates or contact the AppViewX Support Team.
Invalid Create Certificate Payload	Missing or invalid input parameters/ JSON body in the request.	Please validate the input parameters/payload provided or contact the AppViewX Support Team.
Too many create certificate requests	Too many create certificate requests for EJBCA.	Please try to create a certificate request after some time or contact the AppViewX Support Team.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Renewing an EJBCA Certificate

Error Message	Possible Cause	Possible Solution
Error while renewing certificate. - Subject DN field <FieldName> must exist.	FieldName may set as mandatory in the selected End entity profile in EJBCA portal	1. Set the FieldName as optional in the selected End entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (if the field is Organization, Organization unit, Locality, Country, State) If the field is not listed on the enrollment page, add the field in the End entity profile, then pass the value via the enrollment page.
Error while renewing certificate. - Wrong number of <FieldName> fields in Subject Alternative Name.	No. of values sent and no. of values configured for the field do not match.	1. Send the exact number of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal as sending value count.
Error while renewing certificate. - Couldn't find certificate profile (<ProfileId>), among available certificate profiles	Certificate profile selected may not be configured in the selected end entity profile.	Configure the selected certificate profile in the selected end entity profile.
Error while renewing certificate. - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/EJBCA server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but the operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in EJBCA server for creating certificates, or contact AppViewX Support.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for EJBCA.	Please try to create a certificate request after some time or contact AppViewX Support.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available	Use regenerate or upload the private key and perform renew action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating an EJBCA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - Subject DN field <FieldName> must exist.	FieldName may set as mandatory in the selected end entity profile in EJBCA portal.	1. Set the FieldName as optional in the selected end entity profile in EJBCA portal. 2. Add a value for the failed field in the certificate enrollment page (If the field is Organization, Organization unit, Locality, Country, State). If the field is not listed on the enrollment page, add the field in the end entity profile, then pass the value via the enrollment page.
Unable to submit the CSR request to certificate authority - Wrong number of <FieldName> fields in Subject Alternative Name.	No of values sent and number of values configured for the field do not match.	1. Send the exact number of values for the fields configured in the EJBCA portal. 2. Change the field count in EJBCA portal as sending value count.
Unable to submit the CSR request to certificate authority - Couldn't find certificate profile (<ProfileId>,) among available certificate profiles	Certificate profiles may not be configured in the selected end entity profile.	Configure the selected certificate profile in the selected end entity profile
Unable to submit the CSR request to certificate authority - End Entity data contains a CA, <CA ID>, which the Certificate Profile, <ProfileId>, isn't authorized to use.	Configuration of the selected issuer is not done in the selected certificate profile.	Configure the selected issuer name in the selected certificate profile.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	he configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but the operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in EJBCA server for creating certificates, or contact AppViewX Support.
Invalid Create Certificate Payload	Missing or invalid input parameters/JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for EJBCA	Please try to create a certificate request after some time or contact AppViewX Support.

Issues in Revoking an EJBCA Certificate

Error Message	Possible Cause	Possible Solution
Error while revoking certificate-Could not find end entity certificate.	The issuer name in the connector may be wrong	Set the actual issuer name in the connector then perform revoke action.
Missing issuer details in the request.	Issuer details may be missing.	Provide the issuer details.
Unable to establish connection with CA	he configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	AppViewX may not be able to reach the CA.	Check whether network access is available.

Issues in Suspending an EJBCA Certificate

Error Message	Possible Cause	Possible Solution
Error while suspending certificate-Could not find end entity certificate.	The issuer name in the connector may be incorrect.	Set the actual issuer name in the connector then perform revoke action.
Missing issuer details in the request.	Issuer details may be missing.	Provide issuer details.
Unable to establish connection with CA.	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Reinstating EJBCA Certificate

Error Message	Possible Cause	Possible Solution
Error while reinstating certificate-Could not find end entity certificate.	The issuer name in the connector may be wrong.	Set the actual issuer name in the connector then perform revoke action.
Missing issuer details in the request.	Issuer details may be missing.	Provide issuer details.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovering EJBCA Certificates

Error Message	Possible Cause	Possible Solution
Expiry days need to be configured to discover certificates.	Expiry days not configured in the selected EJBCA CA Settings.	Set the expiry days in the selected CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Troubleshooting for Entrust MPKI Issues

This section helps you troubleshoot the common problems that you might encounter when using Entrust MPKI functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Configuring Entrust MPKI CA

Error Message	Possible Cause	Possible Solution
Unable to save CA settings. CA Settings name already exists.	A CA setting with the same name for Entrust MPKI already exists in inventory.	Check the CA setting name, it should be unique.
Fetch certificate types action has failed Proxy details is not configured in proxy settings	Proxy details have not been configured correctly.	Configure valid proxy details.
Unable to establish connection with the CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling an Entrust MPKI Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.-Invalid organization name provided.	Organization information provided might not be available in the CA account.	Please check the list of organizations available in the CA settings.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	Check whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Renewing a Entrust MPKI Certificate

Error Message	Possible Cause	Possible Solution
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating a Entrust MPKI Certificate

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Revoking a Entrust MPKI Certificate

Error Message	Possible Cause	Possible Solution
You must select a Certificate Authority to issue the certificate from	The CA certificateId may be incorrect.	Provide the valid ID of the intermediate certificate authority (ICA) certificate to select as the issuing certificate.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Troubleshooting for GlobalSign CA Issues

This section helps you troubleshoot the common problems that you might encounter when using GlobalSign CA functionalities like setting addition, connectivity, certificate enrollment, renewal, reissue, revocation, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Configuring GlobalSign CA

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for GlobalSign already exists in inventory.	Check the CA Setting name, it should be unique.
This field should not be null or empty	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Mandatory Field(s) - <Field name> is/are empty		
CA Settings - [<Fields>] mandatory fields cannot be empty.		

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
CA Settings name already exists.	A CA setting with the same name for GlobalSign already exists in inventory.	Check the CA Setting name, it should be unique.
Invalid URL	vendorSpecificSettings.url is not valid.	Provide valid input for vendorSpecificSettings.url.
Login should not be blank	vendorSpecificSettings.login is not valid.	Provide valid input for vendorSpecificSettings.login.
Password should not be blank	vendorSpecificSettings.password is not valid.	Provide valid input for vendorSpecificSettings.password.

Issues in Enrolling a GlobalSign CA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.	Invalid credentials.	Check the credentials provided.
	Invalid Global Sign URL.	Check the provided URL.
	IP is not whitelisted by GlobalSign firewall.	Make sure your public IP is whitelisted by GlobalSign.
	Invalid CSR parameters.	Validate the CSR parameters.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings>general.
Invalid Common Name, Please provide valid commonname.	Common name provided in CSR is invalid.	Provide a valid common name in CSR parameters.
Empty response received from the portal, Check with Proxy/CA Setting configurations.	Error in provided CA details.	Check the given CA details.
	Check if the CA portal is accessible from AppViewX.	Check for internet/proxy settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid Validity Period	Validity period provided is invalid.	Check with CA for the supported validity period and update accordingly.

Issues in Renewing a GlobalSign CA Certificate

Issues in Revoking a GlobalSign CA Certificate

Error Message	Possible Cause	Possible Solution
Order ID not provided to get corresponding certificate Id.	Order id is empty in the revoke request.	Check and provide a valid order id.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings > general.

Issues in Discovering GlobalSign CA Certificates

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority.	Invalid credentials.	Check the credentials provided.
	Invalid Global Sign URL.	Check the provided URL.
	IP is not whitelisted by GlobalSign firewall.	Make sure your public IP is whitelisted by GlobalSign.
	Invalid CSR parameters.	Validate the CSR parameters.
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings > general.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Validating GlobalSign CA Connectivity

Error Message	Possible Cause	Possible Solution
Invalid Global Sign Credentials.	Proxy details provided might be incorrect.	Provide valid proxy details.
	Invalid credentials	Please check the credentials provided.
	Invalid GlobalSign URL.	Please check the provided URL.
	IP is not whitelisted by GlobalSign firewall.	Please make sure your public IP is whitelisted by GlobalSign.
Connection failed due to incorrect CA settings details | Access denied due to invalid permissions.	Invalid credentials	Please check the credentials provided.

Issues in Reissuing a GlobalSign CA Certificate

Error Message	Possible Cause	Possible Solution
Host endpoint cannot be null or empty.	Endpoint URL of the given CA setting is null or empty.	Provide valid endpoint URL during CA setting addition.
Proxy details is not configured in proxy settings	Proxy settings are not available.	Configure proxy settings in settings > general.

Troubleshooting for GoDaddy CA Issues

This section helps you troubleshoot the common problems that you might encounter when using GoDaddy CA functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstating, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Configuring GoDaddy CA

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for GoDaddy already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty** • **Mandatory Field(s) - <Field name> is/are empty** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please enter valid credentials – URL	URL entered might be wrong and not in proper URL format	Please check the URL entered

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Issues in Enrolling a GoDaddy CA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may not be available for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may be available for the product type selected in the GoDaddy account but the selected certificate validity may be incorrect for the product purchased.	Edit the CA connector and change the Validity in CSR parameters as purchased in the product.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in GoDaddy server for creating certificates or Contact AppViewX Support.
Invalid Create Certificate Payload	Most likely missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for GoDaddy.	Please try to create a certificate request after some time or contact AppViewX Support.

Issues in Renewing a Godaddy CA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request	Units may not be available for the product	Purchase a valid unit for the product type in the GoDaddy account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
to certificate authority - No available units for the selected product type	type selected in the GoDaddy account.	
Unable to submit the CSR request to certificate authority - No available units for the selected product type	Units may be available for the product type selected in the GoDaddy account but the selected certificate validity may be incorrect for the product purchased.	Edit the CA connector and change the Validity in CSR parameters as purchased in the product.
Unable to submit the CSR request to certificate authority - No orderId available	There might not be any order id i.e certificate id available for the certificate in ca connector information.	• Update the order id manually by copying it from the GoDaddy portal. • Or do the following: 1. Download and have a backup of the certificate. 2. Delete the certificate from the inventory. 3. Do a GoDaddy discovery to get back the certificate id or order id.
Unable to renew the certificate	Renewal of GoDaddy certificates via AppViewX is not supported. GoDaddy handles the auto-renewal of its issued certificates.	1. Enable auto-renewal of certificates on the GoDaddy portal. For instructions, refer the GoDaddy documentation here. 2. Create a scheduled Certificate Authority discovery instance in AppViewX for discovery of the renewed GoDaddy certificates. While enrollment, reissue, regeneration, and revocation of GoDaddy certificates is supported via AppViewX (through the purchase of SSL credits), GoDaddy automatically handles the renewal process. The scheduled discovery

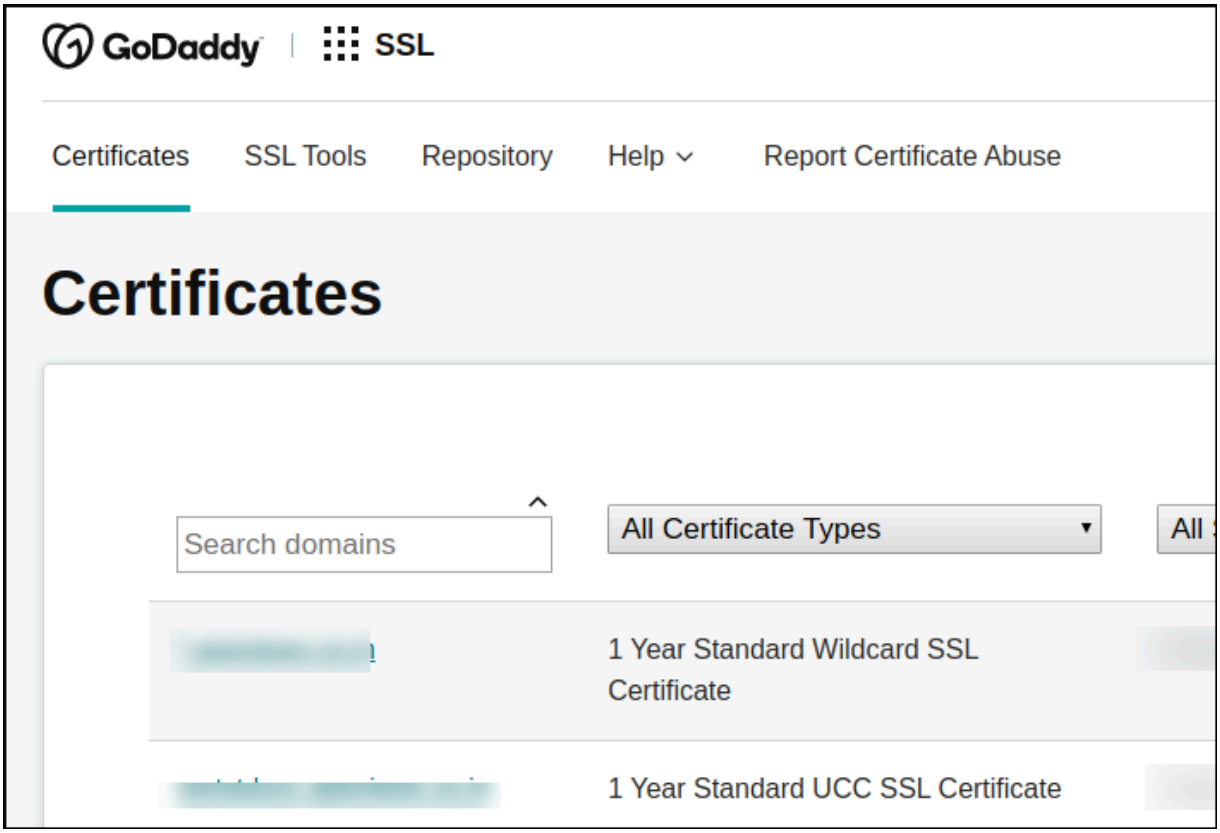
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		instance is to ensure that the renewed certificates are automatically updated in your AppViewX certificate inventory regularly.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/ GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges in GoDaddy server for creating certificates or Contact Support Team.
Invalid Create Certificate Payload	Most likely missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for GoDaddy	Please try to create a certificate request after some time or contact AppViewX Support.

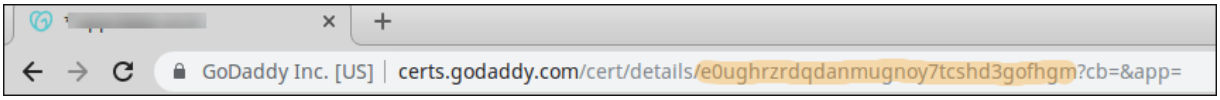
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Retrieving the certificate ID (order ID) from the Go Daddy Portal

1. Login to your GoDaddy account.
2. Navigate to **My Account** > **SSL Certificates**.
   Here you can see the list of certificates created via this GoDaddy account.

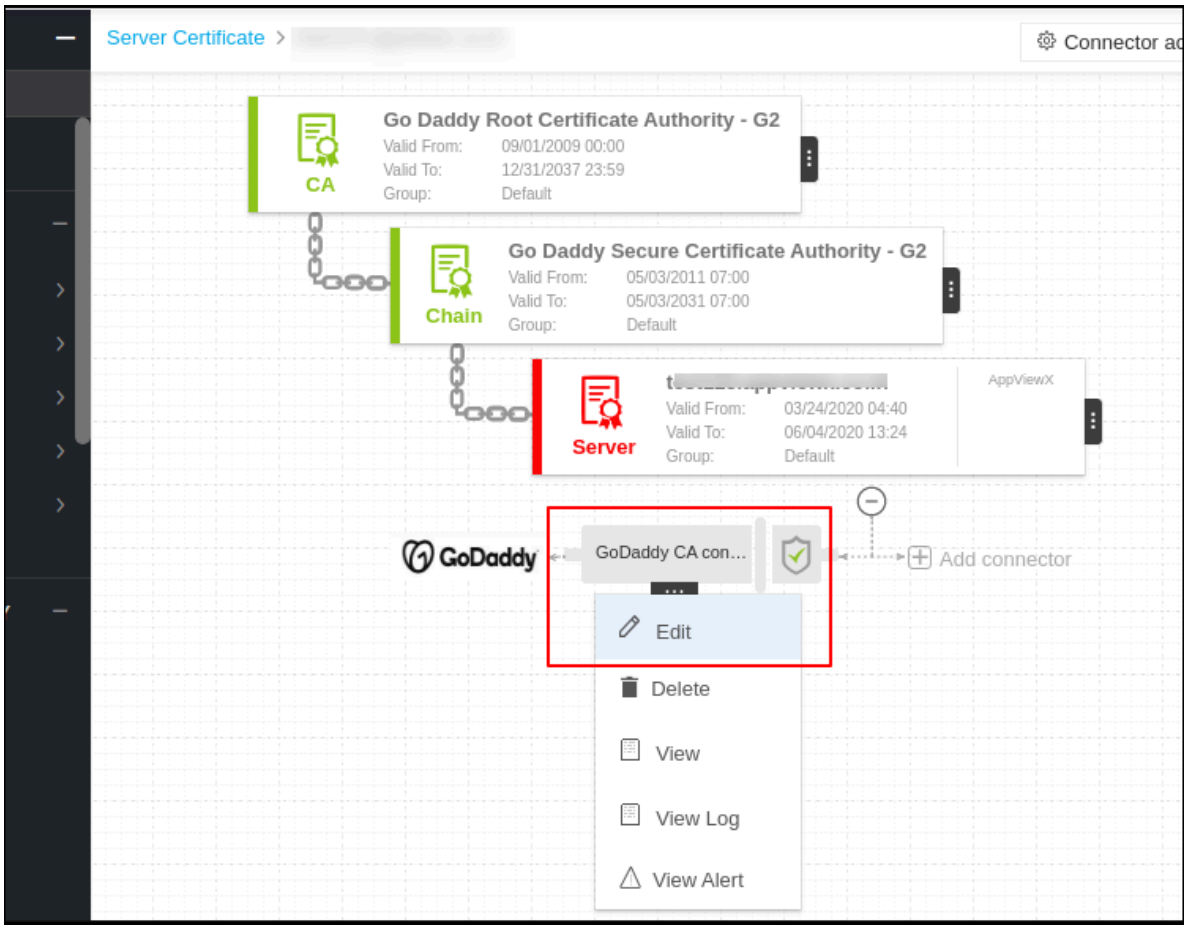


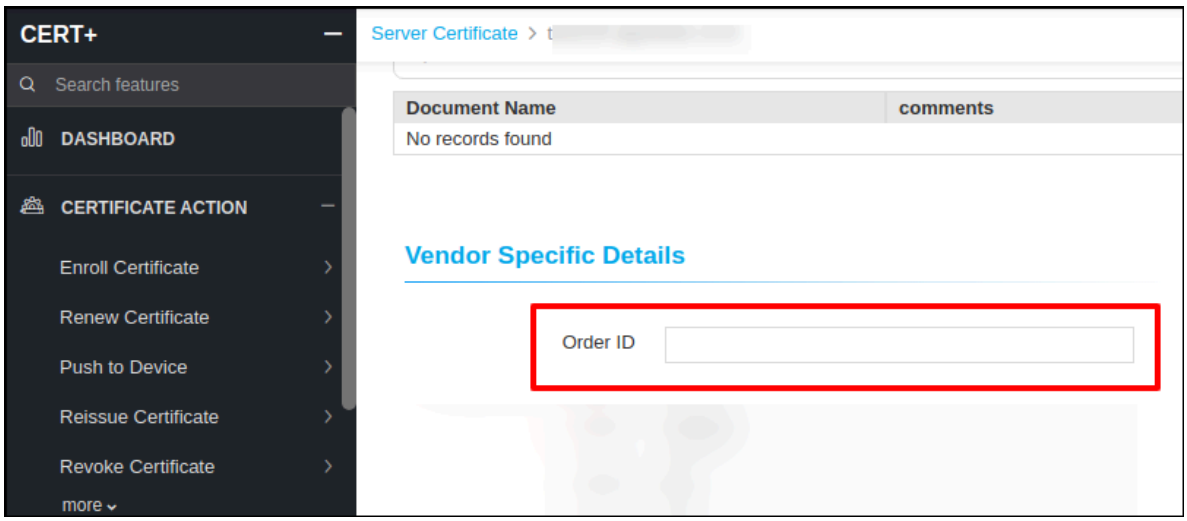
3. Click on the certificate for which you require the order ID.
   In the URL framed you can see the order ID.



4. Use this order ID in our AppViewX CA connector as shown below:
   a. Click on edit in CA connector options.
   b. Find for Order Id in vendor specific fields.
   c. Input the order id obtained from CA portal and update the connector.
   d. Resubmit the failed request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.





Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating a GoDaddy CA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No available units for the selected product type	There might not be available units for the product type selected in the GoDaddy account.	Purchase a valid unit for the product type in the GoDaddy account.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in GoDaddy server for creating certificates or contact AppViewX Support.
Invalid Create Certificate Payload	Missing or invalid input parameters / JSON body in the request.	Please validate the input parameters/ payload provided or contact AppViewX Support.
Too many create certificate requests	Too many create certificate requests for GoDaddy	Please try to create a certificate request after some time or contact AppViewX Support.

Issues in Revoking a GoDaddy CA Certificate

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - No orderId available	There might not be an order id i.e certificate id available for the certificate in ca connector information.	• Update the order ID manually. For instructions, refer the **Retrieving the certificate ID (order ID) from the Go Daddy Portal** here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		• Or do the following: 1. Download and have a backup of the certificate. 2. Delete the certificate from the inventory. 3. Do a GoDaddy discovery to get back the certificate id or order id.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.

Issues in Discovering GoDaddy Certificates

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
Unable to establish connection, Please ensure Proxy/Internet connectivity/ GoDaddy Server.	Invalid proxy details.	Please check the proxy details provided.
	Internet connectivity may not be available.	Please check Internet connectivity to reach CA.
	Invalid URL provided in CA Settings.	Please check whether a valid CA URL is provided in CA Settings or contact AppViewX Support.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Insufficient privilege for the user to create a certificate.	Request accepted but operation is refused due to insufficient privileges, disabled features, etc.	Please refer to the user privileges, disabled features in GoDaddy server for creating certificates, or contact AppViewX Support.

Troubleshooting for Google Private CA Issues

This section helps you troubleshoot the common problems that you might encounter when using Google private CA functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, suspension, and discovery.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Configuring Google Private CA and Google Fetch CA Names

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Google private already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty.** • **Mandatory Field(s) - <Field name> is/are empty.** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling a Google Private CA Certificate

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported keytype or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Renewing a Google Private CA Certificate

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported key type or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available.	Use regenerate or upload the private key and perform renew.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating a Google Private CA Certificate

Error Message	Possible Cause	Possible Solution
Requested entity already exists	certificateId value may be already used to issue a certificate.	Please change the certificateId value to the CA connector. It should be unique.
error parsing CSR: generic::invalid_argument: invalid signature: x509: cannot verify signature: algorithm unimplemented	Unsupported keytype or curve details may be used.	Please check the key type and curve and use valid types.
Certificate authority is not enabled.	Certificate authority may not be enabled in Google portal.	Please enable the selected certificate authority.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Revoking a Google Private CA Certificate

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reason may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Suspending a Google Private CA Certificate

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reasons may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Reinstating a Google Private CA Certificate

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Revocation reasons may not be supported by CA.	Please provide the correct reason.
The requested action is not supported by the issuing CA of the certificate	Selected CA may be in Devops tier.	Please select an Enterprise tier.
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Permission '<Operation>' denied on '<Resource>'	Permission may not be available for the <operation> for the resource.	Please give permission to the user for the specific operation for the resource.

Issues in Discovering Google Private CA Certificates

Error Message	Possible Cause	Possible Solution
Proxy details not configured	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Failed to generate the authentication token	Please check whether the uploaded certificate or JSON is valid.	Invalid client certificate or invalid client Json uploaded.
	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.
Empty response received from the CA.	This URL https://www.googleapis.com may not be reachable.	Please check this URL https://www.googleapis.com can be accessible from the network or whitelist this URL.

Troubleshooting for InCommon CA Issues

This section helps you troubleshoot the common problems that you might encounter while using functionalities like configuration, setting addition, CLM actions and discovery associated with InCommon Certificate Authority.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Configuring InCommon CA

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Unknown user	Username or password may be incorrect.	Check and correct the username and password.
Fetch certificate types action has failed Invalid auth data	URI may be invalid.	Check and correct the URI. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Fetch certificate types action has failed Wrong URL specified or the URL is not reachable	Base URL may be invalid.	Validate and correct the base URL.
Fetch certificate types action has failed Invalid CA settings details	Proxy details could be wrong.	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings of the general

Issues in Enrolling an InCommon CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Regenerating an InCommon Certificate

If a request has failed, then the failure status shall be displayed in the holistic view. Click on the link above the failure message to know the reason for the workflow failure. Common reasons for the failure are mentioned in the table below. Please follow the given remediation steps for the respective error message and resubmit the request.

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Renewing an InCommon Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/	Domain part of the common name specified in the request is	Validate the configured domains or activate the domain in the CA portal, as

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
delegate them or enable this type of certificate for them in terms of the selected organization.	not supported by Certificate Authority	specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Reissuing an InCommon Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Revoking an InCommon Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Issues in Discovering InCommon Certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA Settings.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Troubleshooting for LetsEncrypt CA Issues

This section helps you troubleshoot the common problems that you might encounter while using functionalities like setting addition, connectivity, certificate enrollment, renewal, revocation, and other actions associated with LetsEncrypt.

Supported Web Browsers

Error messages and resolutions

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Devices

Error messages and resolutions

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Configuring Let's Encrypt CA

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings. CA settings name already exists.	A CA setting with the same name for LetsEncrypt already exists in inventory.	Check the CA Setting name, it should be unique.
Please validate given information	Invalid URL given.	Please check the URL.
	LetsEncrypt portal might be down.	Please check any problem in the LetsEncrypt portal.
	Proxy might be required.	Please check the proxy required for this environment. Proxy details may not be configured in proxy settings.
This field should not be null or empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Mandatory Field(s) - <Field name> is/are empty		
CA Settings - [<Fields>] mandatory fields cannot be empty.		
Invalid Email Id	Email ID given while account creation is invalid.	Provide valid email ID.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling a Let's Encrypt CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is invalid.	Provide valid proxy details.
Invalid Authorization	Authorization failed while fetching the challenge.	Provide valid CSR details in the request to receive valid order details in the CA response.
Challenge Not Found	Challenge not received from CA.	Provide valid CSR details in the request to receive valid order details in the CA response.
Error during calculating thumbprint	Invalid public key or publicjsonweb key.	Provide valid details while adding the LetsEncrypt account.
Timeout while Validating Challenge	Challenge verification was not completed within the time limit.	Verify the challenge within the time limit or generate a new challenge and verify.
Challenge Verification Failed	Challenge verification returned status as Invalid from CA.	Check if the internet or proxy is enabled. Check if the TXT record has been added correctly.

Issues in Renewing a Let's Encrypt CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is invalid.	Provide valid proxy details.

Issues in Revoking a Let's Encrypt CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid proxy details specified.	Proxy detail is not configured in proxy settings or is valid.	Provide valid proxy details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Content Extraction Failed	Unable to get encoded X509 certificate using its content.	Provide valid certificate content for the certificate to be revoked.

Issues in Validating Let's Encrypt CA Connectivity

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Communication with CA failed.	Proxy details provided may be incorrect.	Provide valid proxy details.
	Invalid LetsEncrypt Account Id.	Provide valid credentials associated with a valid account.

Issues in Sending REST Requests to Let's Encrypt CA

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
In getKeyStore(), While getting instance for the keystore and loading the store file	Unable to read keystore file “avx_client_cert_keystore” from security path, i.e. $(JAVA_HOME}/lib/security/	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While traversing to java security folder	Java security directory is missing or is corrupted.	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While getting the instance for the keystore	Unable to get Keystore instance.	Internal error. Possibly a deployment issue. Contact support team.
In createStore(), While loading the key store	Unable to load keystore.	Internal error. Possibly a deployment issue. Contact support team.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting for Microsoft Enterprise CA Issues

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstation, discovery, and other actions associated with Microsoft Enterprise.

Issues in Configuring Microsoft Enterprise CA and Fetch CAs

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
• **This field should not be null or empty** • **Mandatory Field(s) - <Field name> is/are empty** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not	Check whether network access is available.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	be able to reach CA.	
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	Kerberos configuration is not configured for the target machine. The most common Kerberos configuration issue is that an SPN with the format HTTP/ <SERVER> is not configured for the target.	The issue occurs with Powershell Remoting since it uses Kerberos Authentication. • In Agent Machine start command prompt as Administrator and execute the following command • setspn –s http/machinename domain\username. • Please note this will work in environments where Kerberos Authentication is set up and there is an AD Domain Setup • If no kerberos authentication is set up then we need to communicate via WMI. • Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. • If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		For more information, see the about_Remote_Troubleshooting Help topic.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) **OR** **Error Code 0x80070005 - Access is denied**	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "`Enable-PSRemoting -force`". 4. Execute "`netsh winhttp show proxy`" and if a proxy is configured then

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		we need to reset it via "netsh winhttp reset proxy". 5. For more information, see the about_Remote_Troubleshooting Help topic.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		• Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Verify that the service on the destination is running and is accepting requests. 5. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. 6. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	The Remote Procedure Call Service	Navigate to the target machine and start RPC service if it has stopped.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	is not responding.	
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig". • Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		(Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
This site can’t be reached	This site can’t be reached.	• Windows Gateway is not reachable from AppViewX. • Windows Gateway service is down.
Html response : Access is denied	Access is denied.	• In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. • Client certificate used in AppViewX is not imported in Target machine's Local computer store.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution

More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator
		1. Check existing config winrm get winrm/config.
		2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring
		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		.

Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request.
This user is allowed a maximum number of 4 concurrent shells, which has been exceeded.
Close existing shells or raise the quota for this user.
	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator
		1. Check existing config winrm get winrm/config.
		2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring
		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'` .
Client Certificate gives Permission Denied 403 error. **This can happen in certain environment and its intermittent**	CA Store mismatch or invalid client certificate used.	Check if the Client certificate is installed correctly by checking the chain in the Personal Store. • Root of the client certificate should be available in the Trusted Root Certification Store of the Server. • Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. • If all the above looks good then go to the agent server and do the following steps 1. MMC. 2. Add “Add/Remove SnapIn. 3. select certificates. 4. select “LocalMachine”. 5. Navigate to the Personal Store and click on the client certificate. 6. Navigate to Chain. 7. Export the Root certificate and save it as Root.cer in a location. 8. Import the “Root.cer” into trusted Root back again.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		9. If the issue still remains unsolved, then check if the Trusted root contains and non-root certificates. 10. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. 11. Take a backup of such certificates and move it to respective stores. 12. If the issue remains unsolved, then add the root certificate to "Client Certificate Issuers".
The permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The user name or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The user name or password is incorrect.	Check if the credentials are valid.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	1. C:\Windows\system32>WinRM quickconfig 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
• **There is not enough space on the disk** • **The WSMan service could not launch a host process to process the given request. Make sure the WSMan provider host server and proxy are properly**	There is not enough space on the disk.	Ensure that your hard disk has enough free space.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
registered. For more information, see the about_Remote_Troubleshooting Help topic. • **Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\ \1jmtip3g.sjl\1jmtip3g.sjl.ps1, Error is, Stack trace Management Cannect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fail within the expected range.**		
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		configured username is part of the administrator group. • or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to agent machine.. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service 9. Remove the username and password from AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling, Renewing, and Regenerating a Microsoft Enterprise CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	Check the CA details configured on the CA settings page. Check whether proxy details are configured in proxy settings. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
The account configured in Application pool identity don't have access to the requested Template	User doesn’t have access	Please give access to the user.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	to the template.	
DATA is invalid log message	Invalid header for CSR.	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available.	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials. 3. To verify template name, Go to CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it, and select properties, In General Tab, you can find Template name which needs to be used in AppViewX. 4. To check Template permission, Go to the CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it and select

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		properties, in the security tab check all permissions given for the user.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority.	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if dll is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to Local Users and Groups and access

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group.
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right-click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has the necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps: a. MMC. b. Add “Add/Remove SnapIn. c. select certificates. d. select “LocalMachine”. e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		g. Export the Root certificate and save it as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find service "AppViewXCertPlus" 4. Right-click and view properties. 5. Click on "log on" tab

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a popup message will appear and ask you to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
CSR Parameters invalid error	CSR Parameters supplied mismatch with Selected template/CA's Policy.	Supply valid CSR values accepted by template or CA policy.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Incorrect certificate template used.	Use template name instead of the template display name.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the	Powershell remoting is not configured.	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Revoking Microsoft Enterprise certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Suspending Microsoft Enterprise certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Reinstating Microsoft Enterprise certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovering Microsoft Enterprise certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Troubleshooting for Microsoft Standalone CA Issues

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstation, discovery, and other actions associated with Microsoft Standalone.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Microsoft Standalone CA Setting Addition and Fetch CAs

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty	Some of the mandatory	Add all the valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	fields might be missing or might be invalid.	
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the	Kerberos configuration is not configured for target machine	The issue occurs with “Powershell Remoting” since it uses Kerberos Authentication 1. In Agent Machine start command prompt as Administrator and execute the following command. 2. `setspn –s http/machinename domain \username.` 3. Please note this will work in environments where Kerberos

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic		Authentication is setup and there is an AD Domain Setup. 4. If no kerberos authentication is set up then we need to communicate via WMI.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied	1. The username should be configured as "Username@Domain" 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of administrator group
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". Execute "netsh winhttp show proxy"

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the	Powershell remoting is not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
destination to analyze and configure the WinRM service: "winrm quickconfig"		
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	Remote Procedure Call Service is not responding	Navigate to the target machine and start RPC service if it has stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. 4. Check if WinRM service is running. 5. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 6. Execute "Enable-PSRemoting -force".
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		3. Navigate to local Users and Groups and access "Administrators". 4. Check if the configured username is part of the administrator group.
This site can’t be reached	This site can’t be reached	1. Windows Gateway is not reachable from AppViewX. 2. Windows Gateway service is down.
Html response : Access is denied	Access is denied	1. In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should have intermediate certificates only. 2. Client certificates used in AppViewX are not imported in Target machine's Local computer store.
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator. 1. Check existing config. 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'. • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'. • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config. 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'. • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'. • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	CA Store mismatch or invalid client certificate used	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to agent server and do following steps a. MMC. b. Add “Add/Remove SnapIn. c. select certificates. d. select “LocalMachine” e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on “Trusted Root” store and check if there are any certificates which have different IssuedTo and IssuedBy. k. Take backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	Certification Authority database has too many active sessions	In CA server navigate to registry via regedit command and set the following 1. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount to 64 hex (100 Dec) 2. HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The username or password is incorrect	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect	The username or password is incorrect.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that	Powershell remoting is not configured	C:\Windows\system32>WinRM quickconfig

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
1. There is not enough space on the disk 2. The WSMan service could not launch a host process to process the given request. Make sure the WSMan provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic. 3. Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\ \1jmtip3g.sjl\1jmtip3g.sjl.ps1, Error is, Stack trace Management Cannect to remote machine mspwvadsnybcc01.csc.nycnet as user failed	There is not enough space on the disk	Ensure that your hard disk has enough free space.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
with the following error Value does not fail within the expected range.		
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn’t have access to CA. Please change the logon credentials in service.	1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right click and view properties. 5. Click on "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add an account as "Log on as service". Click "OK" and save the changes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		8. Click on restart the service. 9. Remove the username and password from AppViewX.

Issues in Enrolling, Fetching, Renewing, and Regenerating Microsoft Standalone Certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	mixed type certificates. 2. Client certificate may be wrong.	certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
DATA is invalid log message	Invalid header for CSR	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if DLL is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. 3. Navigate to local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	Certification Authority database has too many active sessions	In CA server navigate to registry via regedit command and set the following 1) `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec) 2) `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec)
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		4. Execute "netsh winhttp show proxy" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. **This user is allowed a maximum number of 4 concurrent shells, which has been exceeded.** **Close existing shells or raise the quota for this user.**	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring. • winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}' • winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}' • winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'
Client Certificate gives Permission Denied 403 error. **This can happen in certain environment and its intermittent**	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to agent server and do following steps: a. MMC . b. Add “Add/Remove SnapIn c. select certificates. d. select “LocalMachine”. e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain. g. Export the Root certificate and save as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on “Trusted Root” store and check if there are any certificates which have different IssuedTo and IssuedBy. k. Take backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers"
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		3. Find the service "AppViewXCertPlus". 4. Right click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will popup to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured	1. C:\Windows\system32>WinRM quickconfig. 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		• WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Revoking a Microsoft Standalone Certificate

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Suspending a Microsoft Standalone Certificate

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Reinstating Microsoft Standalone certificate

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement	Please use the correct reason which is supported by the CA
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovering Microsoft Standalone certificates

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid

Troubleshooting Sectigo CA

This section helps you troubleshoot the common problems that you might encounter while using functionalities like setting addition, certificate enrollment, renewal, revocation, discovery, and other actions associated with Sectigo Certificate Authority.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Sectigo CA Configuration

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Fetch certificate types action has failed Unknown user	Username or password may be invalid	Check and correct the username and password.
Fetch certificate types action has failed Invalid auth data	URI may be invalid	Check and correct the URI. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Fetch certificate types action has failed Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Fetch certificate types action has failed Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Sectigo CA setting validation

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be in valid	Check and correct the username and password.
Invalid auth data	URI may be invalid	Check and correct the URI. For example: https://cert-manager.com/customer/

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		<customer_uri>/ssl - here URI is customer_uri.
Connection failed due to incorrect CA settings details : Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL.
Connection failed due to incorrect CA settings details : Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the general settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA settings but proxy details are not configured in proxy settings.	Configure the proxy details in general settings.

Issues in Enrolling Sectigo Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating Sectigo Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/	Domain part of the common name specified in the request is	Validate the configured domains or activate the domain in the CA portal, as

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
delegate them or enable this type of certificate for them in terms of the selected organization.	not supported by Certificate Authority	specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Renewing Sectigo Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/ delegate them or enable this type of certificate for them in terms of the selected organization.	Domain part of the common name specified in the request is not supported by Certificate Authority	Validate the configured domains or activate the domain in the CA portal, as specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Reissuing Sectigo Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.
You cannot order certificates for the following or additional domains: testcert.test.net. Please double-check correctness of entered information or navigate to "Domains" subtab of "Settings" tab to request/activate/	Domain part of the common name specified in the request is	Validate the configured domains or activate the domain in the CA portal, as

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
delegate them or enable this type of certificate for them in terms of the selected organization.	not supported by Certificate Authority	specified in the error message.
The validity period (term) is invalid for this certificate type.	The validity period (term) is invalid for this certificate type.	Please specify the validity period (term) that is supported by the chosen cert type in the CA connector and resubmit the request.
Certificate Profile does not support Key Type 'EC - brainpoolP160r1'.	EC key type with the specified curve is not supported for the chosen certificate type.	Please specify the key type that is supported by the chosen cert type in the CA connector and resubmit the request.

Issues in Revoking Sectigo Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Issues in Discovering Sectigo Certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unknown User	Username or password may be invalid	Check and correct the username and password in the CA setting.
Invalid auth data	URI may be invalid	Check and correct the URI in the CA setting. For example: https://cert-manager.com/customer/<customer_uri>/ssl - here URI is customer_uri.
Wrong url specified or the url is not reachable	Base URL may be invalid	Validate and correct the base URL in the CA Settings.
Invalid CA settings details	Proxy details could be wrong	Check and correct the proxy details configured in the proxy settings.
Proxy details is not configured in proxy settings.	Proxy field is enabled in CA Settings but proxy details are not configured in proxy settings.	Configure the proxy details in proxy settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Symantec CA

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, reissue, and other actions associated with Symantec CA.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Symantec CA setting addition and fetch custom attributes

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Symantec already exists in inventory.	Check the CA Setting name, it should be unique.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
1) This field should not be null or empty 2) Mandatory Field(s) - <Field name> is/are empty 3) CA Settings - [<Fields>] mandatory fields cannot be empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
<Field> should not be blank	Mandatory field <Field> may be missing	Please add the field <Field> and proceed
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid	Use the valid certificate

Issues in Enrolling Symantec certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Fetching Symantec certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings.	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Renewing Symantec certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX	Please configure proxy details in AppViewX
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available	Use regenerate or upload the private key and perform renew.

Issues in Regenerating Symantec certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Revoking Symantec certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Issues in Reissuing Symantec certificate

Error messages and resolutiosn

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
The SSL certificate error	Used certificate may be invalid.	Use the valid certificate.

Troubleshooting Trustwave CA

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, regeneration, revocation, reissue, and other actions associated with Trustwave CA.

Supported Web Browsers

Error messages and resolutions

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Browser	Version	Notes
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Error messages and resolutions

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Trustwave CA Setting Addition

Error messages and their resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Trustwave already exists in inventory.	Check the CA Setting name, it should be unique.
1) This field should not be null or empty **2) Mandatory Field(s) - <Field name> is/are empty**	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and their resolutions (continued)

Error Message	Possible Cause	Possible Solution
3) CA Settings - [<Fields>] mandatory fields cannot be empty.		
<Field> should not be blank	Mandatory field <Field> may be missing.	Please add the field <Field> and proceed.
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Authentication failed for user <user>	Username or password may be wrong	Please provide the valid username and password
Authorization failed	Incorrect reseller id provided	Please provide valid reseller id.
You don't have permission to access <url> on this server.	Invalid URL specified.	Please provide a valid URL.

Issues in Enrolling Trustwave Certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Unsupported certificate type {certType} with validity year : {year}	Certificate type selected may be invalid.	Please select the valid certificate type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
The following name(s) do not end with a top level domain registered in IANA's Root Zone Database: <commonName>	Specified common name is invalid , it should end with a domain name.	Please provide a valid common name.

Issues in Fetching Trustwave Certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Certificate is not issued	Certificate polling may be in progress.	Certificate polling will happen and retrieve once the certificate is issued.

Issues in Renewing Trustwave certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order ID not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.
CSR or private key is not available. Use the regenerate option.	CSR or private key may not be available.	Use regenerate or upload the private key and re- perform renew.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Regenerating Trustwave certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX
Unsupported certificate type {certType} with validity year : {year}	Certificate type selected may be invalid.	Please select the valid certificate type.
The following name(s) do not end with a top level domain registered in IANA's Root Zone Database: <commonName>	Invalid common name specified, it should end with a domain name.	Please provide a valid common name.

Issues in Revoking Trustwave certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Proxy details is not configured in proxy settings	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order ID not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.

Issues in Reissuing Trustwave certificate

Error Message	Possible Cause	Possible Solution
Proxy details are not configured in proxy settings.	Proxy details may not be configured in AppViewX.	Please configure proxy details in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Proxy authentication configuration in proxy settings could be wrong	Proxy details configured in AppViewX may be invalid.	Please configure valid proxy details in AppViewX.
Order Id not provided to get corresponding certificate Id.	Order id may not be available in the CA connector.	Please update the order id in the CA connector and proceed.
CSR content is empty	CSR may not be available for the certificate to reissue.	Either CSR or private key should be available in the certificate.

Troubleshooting the Windows Agent Setup

Overview

This section helps you troubleshoot the common problems that you might encounter when using Windows Agent Setup. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on Windows Agent Setup. It helps you understand the importance of installing a validator and the method to do so.

Installing a Validator

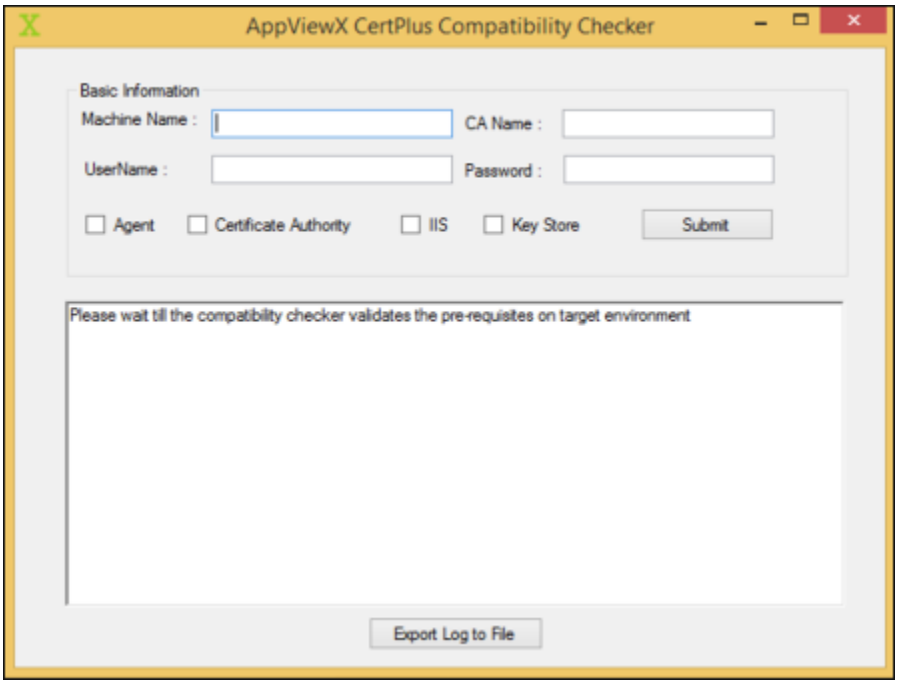
Validator analyzes an Agent and validates all the prerequisites before installing an agent. It is also used to troubleshoot any issue that occurs in the managed machines that run on a network. Before installing AppViewX gateway and the certificates, make sure you have downloaded the validator to either the Downloads folder or to the Desktop in your local environment.

1. Click the AppViewX.CertPlus.Validator.exe file to open the application for validation.
2. In the AppViewX CertPlus Validator screen that opens enter all the mandatory fields in the Basic Information section to proceed.
3. Select the Agent, Certificate Authority, IIS, and Non-IIS checkbox depending on what you want to validate and manage in the target machine.

• Based on the checkboxes you selected, the fields that are mandatory will be highlighted in Red color.
• The CA Name is required only if the Certificate Authority check box is selected.

Click Submit and the results are displayed as shown in the following image:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- AppViewX CertPlus Compatibility Checker is used for troubleshooting or validating the prerequisites as part of Windows Agent Installation. It comprises the following fields:

Name	Description	Condition
Machine Name	The name of the target machine must be validated. It is a hostname.	Mandatory field
CA Name	The name of the CA in the CA config.	Mandatory only when a CA is selected
User Name	User Name to be used for validating the target machine. It is in the format "username@domainname".	Mandatory field
Password	The password corresponding to the provided user name.	Mandatory field

Options

- User can select single or multiple options based on the installation/ troubleshooting criteria:
- Agent: Select this option if we need to install an agent in the target machine which is configured in the "Machine Name". It will validate the prerequisites which are required for Agent Installation
- Certificate Authority: Select this option if we need to validate the Certificate Authority related functionality. The CA Name is mandatory only in this case. Use the certutil -dump command to get the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

CA Name. In the output of certutil command use-value in the "Server" as the Machine Name and use "Name" as the CA Name.

- Based on the example below the machine Name is win3.avxdevlab.net and CA Name is avxdevlab-WIN3-CA-no-space.
- IIS: Select this option if we need to validate the IIS sites related functionality.

Validations

Validate	Agent	CA	IIS	Keystore
User	Yes	Yes	Yes	Yes
.Net framework	Yes	Yes	Yes	Yes
Powershell	Yes	Yes	Yes	Yes
CertUtil	Yes	Yes	No	No
Certadm.dll	Yes	Yes	No	No
netsh	Yes	No	No	No
RPC	Yes	Yes	Yes	Yes
WinRM	Yes	Yes	Yes	Yes
WMI	Yes	Yes	Yes	Yes
IIS	No	No	Yes	No

- **KeyStore**: Select this option if you need to add to validate only the Microsoft Certificate Store related functionality

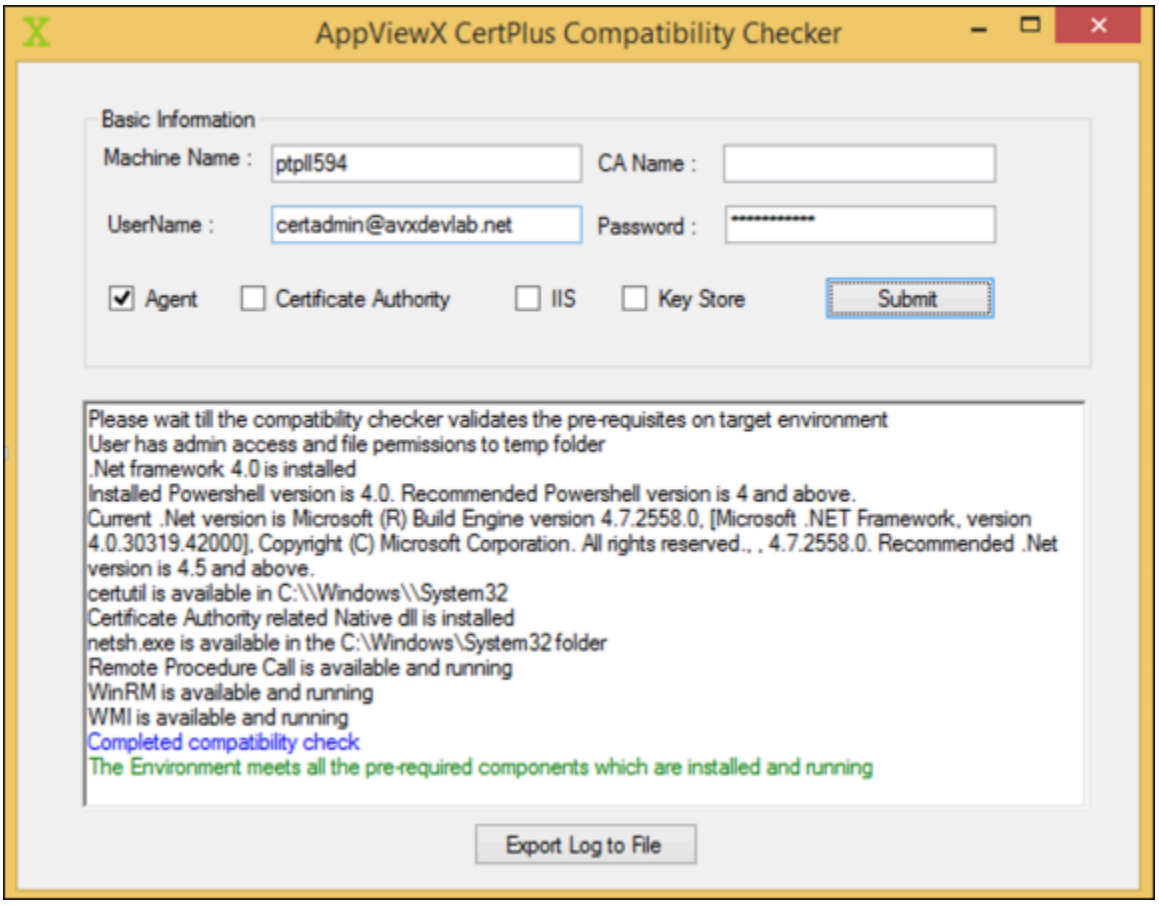
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. User Access: It will validate by connecting to the target machine with the specified username and password and check if it has admin access.
2. .Net Framework: It will check if .Net framework 4.5+ is installed and will display the current .Net framework version.
3. Powershell version: It will check if Powershell is installed and will display the current Powershell version
4. CertUtil: It will check if certutil component is available. This is used to get the CA name and the corresponding templates.
5. CertAdm.dll: This is the native component used to access the CA and will check if this component is available in the C:WindowsSystem32 folder. Sometimes, while trying to access this component during the verification it will return an error and hence, a manual check must be performed.
6. netsh.exe: This is used to bind the certificate to the installed agent port (8999).
7. RPC service: The remote procedure call service must be running to perform all the remote operations and it will validate if the service is installed and running on the target machine.
8. WinRM service: Windows Remote Management service is required for the Powershell execution and it will validate if the service is installed and running on the target machine.
9. WMI service: Windows Management Instrumentation service is required for WMI and Powershell execution and it will validate if the service is installed and running on the target machine.
10. IIS: It will check if the IIS server is installed and identify the current IIS version.

Color Codes during the Execution

- **Black**: Success information and output
- **Red**: An error or warning, must take corrective action based on the prerequisite document in case of any issues
- **Blue**: Completion of the validation process
- **Green**: Complete process is successful

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Export Log to File: This is used for exporting the validation summary into a log file.

Steps to test gateway installation:

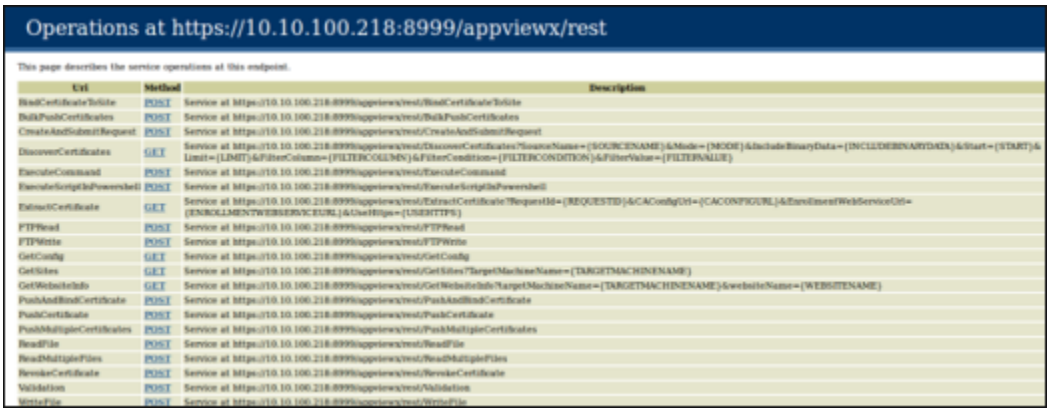
To test the installation, go to the following URL:

https://localhost:8999/appviewx/

`https://<IP/Hostname>:<Port>/appviewx/rest/help` (Needs the certificate to be on the store/ browser)

For example, https://xx.xx.xx.xx:8999/appviewx/rest/help

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



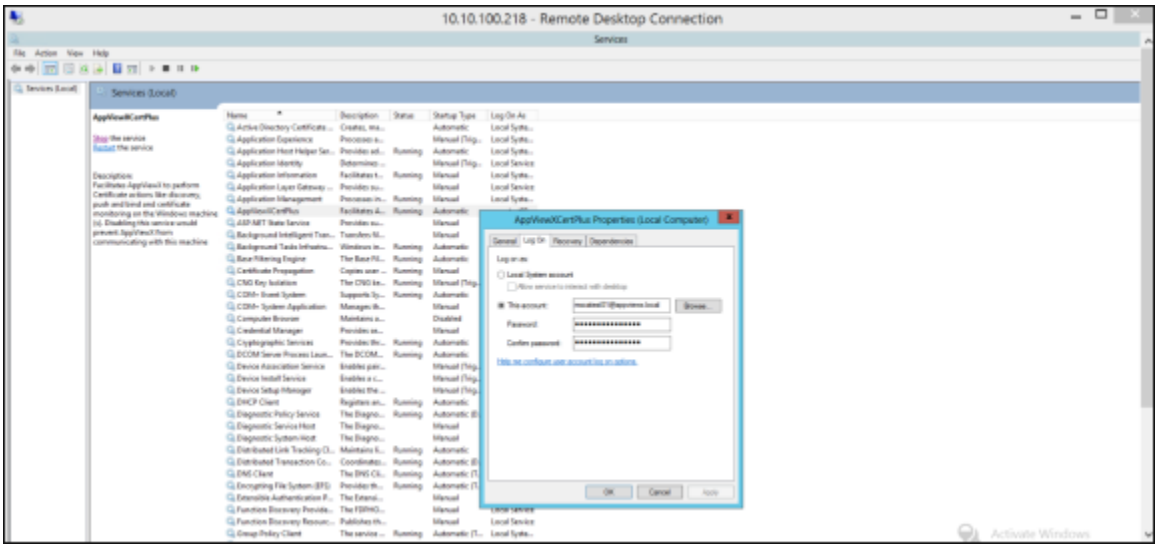
- The above page confirms the accessibility and installation of the service.
- In case, a different client authentication certificate is being used, ensure that the CRL mentioned in the certificate is reachable from the AppViewX Windows gateway hosting server.
- Go to **AppViewX>> Settings>> Certificate** to register the gateway with AppViewX.
- Register the gateway with the URL format as follows: `https://<IP/Hostname>:<Port>/appviewx`

For example, https://xx.xx.xx.xx:8999/appviewx

Modify Agent services with the service Account The Windows gateway agent can be installed using a service account or an admin account.

- If the customer has a policy that states that the service account cannot be part of the administrator group or that the service account is only a part of the user group, then:
  - The gateway agent service is installed using an admin account.
  - The installed agent service is updated with the service account details in services.msc. Add the account in the properties of the AppViewXCert Plus service.
  - Services.msc -> AppViewXCert Plus -> Right click (Properties) -> LogOn .> Update the user account in the format of username@domainname.
  - Refer to the following image.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



- In this case, the following command has to be executed from the PowerShell:

Netsh http add urlacl url=https://+:8999/appviewx/user=appviewx.localmscatest01

- In the above command, the value for user = <domainserviceaccount> and the URL must be changed respectively.
- Once this is done, stop and start the AppViewXCertPlus Service in services.msc.

Windows Gateway Errors and Solutions

Error	Solution
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <machine name> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <name> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command `setspn -s http/machinename domainusername`. • This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the format HTTP/<machine name> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
about_Remote_Troubleshooting Help topic.	
Retrieving the COM class factory for remote component with CLSID	• The component used for accessing CA (certadm.dll) is not installed or has permission issues. • Check if the DLL is available in `C:WindowsSystem32` folder or else, install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. For example, for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
Connecting to remote server <machine name> failed with the following error message: WinRM cannot process the request. The following error with error code 0x80090322 occurred while using Negotiate authentication: An unknown security error occurred.	• This issue occurs with Powershell remoting as it uses Kerberos authentication. • In the agent machine, start the command prompt as an administrator and execute the command `setspn -s http/machinename domainusername`. • This will work in the environments where Kerberos authentication and an AD domain are set up. • If no kerberos authentication is set up, then the communication must be done through WMI.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the	• Check if the WinRM service is running. • Go to the Powershell on the target machine and run the command `WinRM QuickConfig`.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
about_Remote_Troubleshooting Help topic	• Execute the command `Enable-PSRemoting -force`. • Execute the command `netsh winhttp show proxy` and if a proxy is configured, it must be reset using the command `netsh winhttp reset proxy`.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <machine name> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command `WinRM QuickConfig`. • Execute the command `Enable-PSRemoting -force`.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	• Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command `WinRM QuickConfig`. • Execute the command `Enable-PSRemoting -force`.
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable.	Go to the target machine and start the RPC service if it is stopped.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
0x800706ba (WIN32: 1722 RPC_S_SERVER_ UNAVAILABLE)	
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be a part of the local administrator group. • Go to the Local Users and Groups and access "Administrators" and check if the configured username is part of the administrator group. • Check if the WinRM service is running. • Go to Powershell on the target machine and execute the command `WinRM QuickConfig`. • Execute the command `Enable-PSRemoting -force`.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path '\\<machine name>\C$\ \Windows\\Temp\\qgwwkqi3.fff' is denied.	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.

More than 5 connections are not allowed	• Run Powershell as an administrator.
	• Check existing config `winrm get winrm/config`.
	• Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring.
	  • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
	  • `winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
	  • `winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`

Connecting to remote server failed with the following error message: The WS-Management service cannot process the	• Run Powershell as an administrator. • Check existing config `winrm get winrm/config`.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	• Change the settings to increase the maxshellsperUser to 100 on the remote machine where this issue is concurring. • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'` • `winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'` • `winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
Client Certificate gives Permission Denied 403 errors. This can happen in a certain environment and it's intermittent	• Check if the client certificate is installed correctly by validating the chain in the Personal Store. • The root of the client certificate must be available in the Trusted Root Certification Store of the server. • The intermediate of the client certificate must be available in the Intermediate Certification authorities of the server. • If all of the above are fine, go to the agent server and complete the following steps: 1. MMC 2. Add/Remove SnapIn 3. Select certificate 4. Select LocalMachine 5. Go to Personal Store and click on client certificate 6. Go to chain 7. Export the root certificate and save as Root.cer in a location 8. Import the Root.cer into trusted root back again 9. If this does not solve the issue, then check if the trusted root contains and non- root certificates 10. Click on "Trusted Root" store and check if there any certificate which has IssuedTo and IssuedBy different 11. Take a backup of such certificates and move it to respective stores 12. If it does not solve the issue, then add the root certificate to the "Client Certificate Issuers"
The permission on the certificate template do not allow the current user to enroll for this type of certificate	1. Go to the CA server. 2. Open Certificate Authority and select the CA Server. 3. Right-click on properties and select the Security tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
	4. Check if the user used in Agent has the necessary permissions to read, issue, manage, and request certificate(s). 5. If the user is a part of a group, then ensure that the group has the required permissions. 6. Click on the Certificate Templates and right-click to manage the template. 7. Right-click on the template which has the issue and navigates to security. 8. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib. IenumCERTVIEWROW.Next().	In the CA server, navigate to the registry through the regedit command and set the following: 1. HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBSessionCount to 64 hex (100 Dec) 2. HKLMSYSTEMCurrentControlSetServicesCertSvc ConfigurationDBMaxReadSessionCount is also set to 64 hex (100 Dec)
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.rn	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group.
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server <machine name> failed with the following error message : The user name or password is incorrect. For more information, see the	The user name or password is incorrect.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
about_Remote_Troubleshooting Help topic.	

Connecting to remote server <machine name> failed with the following error message: WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits accesses to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	• WinRM service is already running on the following location of the machine: C:Windowssystem32>WinRM quickconfig
	• If WinRM is not set up to allow remote access to this machine for management, the following changes must be made:
	  • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
	  • Make these changes [y/n]? y

There is not enough space on the disk	Ensure that your hard disk has enough free space.
Management Connect to remote machine <machine name> as user failed with the following error User credentials cannot be used for local connections	• The username must be configured as "Username@Domain". • The user must have admin access to the remote/target machine or must be part of the local administrator group. • Go to the Local Users and Groups and access "Administrators". Check if the configured username is a part of the administrator group. • Configure the credentials in AppViewX.CertPlus.Service Logon option.
Denied by Policy Module 0x80094800, The request was	Use template name instead of the template display name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error	Solution
for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	
Device Communication failed while using Native option to connect to CA remotely	1. Go to the agent machine. 2. Open `services.msc` using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add the account as "Log on as service". Click "OK" and save changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
Certificate Request (CSR) is using a different account to request a certificate from CA as compared to account configured in AppViewX	1. Go to the agent machine. 2. Open `services.msc` using Start > Run command on the Windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click on the "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add the account as "Log on as service". Click "OK" and save changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting General

This section of the guide will help you address the general issues faced during various processes related to Certificates like Group, Policy, Reports, and workflow. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

- Troubleshooting Certificate Group
- Troubleshooting Certificate Policy
- Troubleshooting Certificate Reports Configuration
- Troubleshooting Configuration of Workflow
- Troubleshooting Truststore Bundle Deployment

Troubleshooting Certificate Group

Issues in Creating/Updating a Group

Error Message	Possible Cause	Possible Solution
Given parent group is not present in AppViewX.	The parent group provided by the user does not exist in AppViewX.	Check if the group exists in the given parent group name.
Group already exists with the given name	Another group with the same name already exists.	Group name should be unique.
Missing user information.	User information is not available in the request.	Provide valid user information in the request.
Permission restricted to this group to edit/delete.	Given group has only read permission.	Change the group permission as RW to update the group.
Parent name and group name should not be same. Kindly change the parent name.	Parent group name and group name are the same in the given request.	Change the group name in the request.
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Failed to update certificate group.	AppViewX is not able to update the group details.	DB may not be accessible during that time.
Given child group is not present in AppViewX.	The Child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Certificate policy updation failed while updating certificate group.	AppViewX is not able to update the group details in policy.	DB may not be accessible during that time.

Issues in Deleting a Group

Error Message	Possible Cause	Possible Solution
Default group cannot be deleted.	The user is trying to delete the default group provided by AppViewX.	AppViewX allows users to delete only user-defined groups.
Permission restricted to this group to edit/ delete.	Given group has only read permission.	Change the group permission as RW to update the group.
Given parent group is not present in AppViewX.	The parent group provided by the user is not available in AppViewX.	Check if the group is available in the given parent group name.
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
Given child group is not present in AppViewX.	The child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Failed to delete certificate groups since it is not available. Those groups are <GroupNames>	Given groups are not available in AppViewX.	Check and provide a valid group name to delete.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Assigning/Unassigning Certificates to a Group

Error Message	Possible Cause	Possible Solution
You don't have access to this group.	Users do not have permission for a given group.	Change the group permission as RW to update the group.
The operation cannot be completed as <count> selected certificate(s) are in Read-Only access groups	Some of the selected certificates are in groups that have “read-only” permission for the user.	Remove the certificates that have “read-only” permission or Change the group permissions to “RW”.
Group name cannot be empty.	Group is given as empty in the request.	Groupname should not be empty. Give a valid group name.
Certificate uuid either empty/ invalid.	Certificate UUID is not given in the request.	Provide a valid certificate UUIDs to perform the action.

Troubleshooting Certificate Policy

This section of the guide will help you troubleshoot the common problems that you might encounter while dealing with Certificate Policy actions like creating or updating or deleting.

Issues in Creating/Updating a Policy

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
[group] Groups are already assigned to another policy or doesn't exist	The group may be associated with some other policy. Group may not be available in AppViewX.	Check if the group is associated with some other policy. Check if the group is available in AppViewX.
At least one ECDSA curve should be selected for each EC bitlength	ECDSA curve details are not provided in the request.	It is mandatory to give at least one ECDSA curve for each EC bit length.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Failed to fetch the policy.	AppViewX is not able to fetch policy details from DB.	DB may not be accessible during that time. Please retry the operation.
Policy already exists with the given name.	Policy name already exists in the inventory.	Policy names should be unique.
Failed to update certificate policy information.	AppViewX is not able to update policy details from DB.	DB may not be accessible during that time. Please retry the operation.
Given child group is not present in AppViewX.	The Child group provided by the user is not available in AppViewX.	Check if the group is available in the given child group name.
Certificate policy updation failed while updating certificate group.	AppViewX is not able to update the group details in policy.	DB may not be accessible during that time.

Issues in Deleting a Policy

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Default policy cannot be deleted.	The user is trying to delete the default policy provided by AppViewX.	AppViewX allows users to delete only user-defined policies.
Mandatory field is missing or invalid - policyNames	The field policyNames is not provided with any values in the request.	Check if the policyNames field is available and has values in the request.
Failed to delete certificate policy information.	AppViewX is not able to delete the policy.	DB may not be accessible during that time. Please retry the operation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Certificate Reports Configuration

This section of the guide helps you troubleshoot the common problems that you might encounter while configuring various certificate reports like validation status reports, summary reports, count by issuer reports.

Issues in Configuring the Validation Status Report

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
FQDN cannot be null or empty.	The FQDN value provided is either null or empty.	Provide a valid FQDN value.
Certificate network discovery plugin may not be enabled. Contact AppViewX support team.	The plugin avx_vendor_cert_network_discovery is not enabled.	Enable avx_vendor_cert_network_discovery plugin.
Certificate network discovery plugin may be in not running state.	The plugin avx_vendor_cert_network_discovery may be in the “Not Running” state.	Start avx_vendor_cert_network_discovery plugin and try again.
IP <ipPort> is invalid	Given IP port is not valid.	Check and provide a valid IP port.
Invalid FQDN.	AppViewX is not able to access the given FQDN.	Check if the FQDN is valid and whether AppViewX has access to the FQDN.
Missing user information.	User information is not available in the request.	Provide a valid session-id or username and password in the request.

Issues in Configuring the Certificate Summary Report

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Cert report settings name already exists, Please verify.	The report settings name provided is already taken.	Report settings name should be unique.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Unable to schedule report generation, skipping to add/update the settings.	AppViewX is not able to add/ update the scheduler job in crontab.	1. Provide valid cron settings. 2. DB may not be reachable, try after some time.

Issues in Configuring the Count by Issuer Report

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Cert report settings name already exists, Please verify.	The report settings name provided is already taken.	Report settings name should be unique.
Unable to schedule report generation, skipping to add/update the settings.	AppViewX is not able to add/ update the scheduler job in crontab.	1. Provide a valid cron setting. 2. DB may not be reachable, try after some time.

Troubleshooting Configuration of Workflow

This section of the guide helps you troubleshoot the problems encountered while configuring workflow.

Issues in Configuring a Workflow

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Csr submission failed. User is not authorized.	No permission for the workflow related to that action.	Check if the user has permission for the action workflow in Accounts>Resources.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Certificate <action>failed. User is not authorized.	No permission for the workflow related to that action.	Check if the user has permission for the action workflow in Accounts>Resources.

Troubleshooting Truststore Bundle Deployment

Linux Server Bulk Push

Work Order Failure

Error Message	Possible Cause	Possible Solution
Error occurred while changing the file ownership : chown: invalid user: <username:username>	Invalid username for the chown action	Provide a valid username.
Error occurred while changing the file ownership : chown: invalid group: <usergroup:usergroup>	Invalid user group for the chown action	Provide a valid user group.
Unable to upload certificate content to the target server	Permission to access the path to push is not granted.	Provide the required permission for the path to push.
Bulk Push failed - com.appviewx.connector.ssh.SSHExcep tion: net.schmizz.sshj.userauth.UserAuthException: Exhausted available authentication methods	Device is not in the managed state	Onboard device in the server inventory with the **Managed** status.
Password given doesn't match with existing JKS certificate file	Invalid jks certificate file password	Provide a valid keystore password.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Work Order Success

Error Message	Possible Cause	Possible Solution
Skipping push operation since no valid certificates are found in the request.	Expired/ Revoked certificates selected for the bulk push operation	Provide valid certificates for the bulk push operation.

ADC F5 Bulk Push

Failure cases in Bulk Push F5

Error Message	Possible Cause	Possible Solution
Please provide information as required.	Possible causes can include: • Process name field is empty. • Process name field contains restricted special characters. • Chain file or bundle name is empty. • Selected devices are empty.	• Ensure no empty values are provided. • Process name can only include alphanumeric characters, spaces, and the following special characters: #,.,-,_ • Chain or bundle name can only include alphanumeric characters, spaces, and the following special characters: .,-,_
java.lang.Exception: {"code":400,"message":"01070712:3: Access check failed for (/Common/default.crt).","errorStack":[],"apiError":3}	Chain file or bundle name is entered as “default/ca-bundle/ca-bundle 1/ca-bundle 2”.	Edit the bulk push entry and modify the chain file or bundle name to enter a value that is not in the default bundle in the F5 device.

Troubleshooting Auto-Enrolment Protocols

This section of the guide helps you to troubleshoot the various issues encountered by you while using different protocol functionalities. The different protocols covered are ACME, EST, MsIntune SCEP, and SCEP. If the problem still remains unresolved please send a request to Technical Support by opening a

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

case with the AppViewX Technical Services team. You can open a case from helpcenter.appviewx.com or send an email to help@appviewx.com.

- Troubleshooting for ACME
- Troubleshooting for EST
- Troubleshooting for MsIntune SCEP
- Troubleshooting for SCEP

Troubleshooting for ACME

Overview

This section helps you troubleshoot the common problems that you might encounter when using ACME functionalities like setting addition, checking communication, enrollment, and revocation.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported ACME Client

• Certbot

• Cert manager

Issues in ACME setting addition and check the settings

Issues in ACME Setting Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **CERT+**.
   The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **ACME**.
   The **Auto Enrollment ACME** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	An ACME setting with the same name already exists in ACME Page.	Check the ACME Setting name, it should be unique.
1. This field should not be null or empty 2. Mandatory Field(s) - <Field name> is/are empty	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
ACME setting is invalid - Agent ip is not reachable	The ACME agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
ACME setting is invalid - Policy is not associated to the provided group	The policy selected might be associated with some other group that is not selected.	Please check whether the selected policy and group are associated with one another.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Auto Enrolling Certificate via ACME

Note: From the client machine hit the auto-enroll call using AppViewX ACME server URL which is displayed on the ACME setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR)	The provided agent IP or agent name is not found in the ACME settings.	Check for the agent IP and agent name in the client machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Agent settings is not found		
Unable to perform ACME account creation/updation operation	ACME is already present or the account is not proper in the client machine.	1. Check whether the account is proper in the client machine. 2. Delete the acme accounts in the client machine and retry.
Unable to perform ACME challenge creation operation	Challenge verification failed before enrolling the certificate.	1. Check for the option selected in the ACME setting if it's HTTP or DNS. 2. Check for the reachability of URL for HTTP challenge verification.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid	1. Check for passwords in BASIC authentication. 2. Check for the nonce and other parameters in DIGACME parameters.
Unable to perform ACME order finalize operation	This phase is used to obtain the CSR and submit it.	1. Check for the input CSR in the request. 2. Check whether the CSR submission is successful in AppViewX.
Unable to obtain the enrolled certificate	The certificate might not be present for the provided transaction id.	Check if the certificate is enrolled or not in AppViewX inventory.
Unable to establish connection with ACME server.	There might be an issue with reaching the AppViewX ACME agent IP from the client.	Check whether the ACME agent IP is reachable from the client machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		Check whether the ACME agent IP is open and can be accessible.
Group policy does not have the given hash function	The requACMEed hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the ACME setting. 3. In the hash function field include the **requACMEed** and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in the logs and failed Work order for the reason of submission failure.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in work order log - “**Denied due to policy module**”	Check for the bit length in the CSR parameters, if it's lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry as below: `"db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})"` **Note:** This would allow multiple CSR’s with the same parameters in the certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting for EST

Overview

This section helps you troubleshoot the common problems that you might encounter when using EST functionalities of CA like setting addition, enrollment, obtaining, and re-enrollment.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Supported EST Clients

- Cisco Routers
- Libest client

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in EST setting addition and check the settings

Issues in EST setting Addition

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **CERT+**.
   The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **EST**.
   The **Auto Enrollment EST** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	An EST setting with the same name already exists on EST Page.	Check the EST Setting name, it should be unique.
1. This field should not be null or empty. 2. Mandatory Field(s) - <Field name> is/are empty.	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
EST setting is invalid - Agent ip is not reachable	The EST agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.
EST setting is invalid - Certificate does not belong to the selected CA.	The issuer certificate provided does not belong to the CA which is selected.	Please check whether the selected issuer certificate belongs to the CA which was selected earlier.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in auto-enrolling certificate via EST

Note: From the client machine hit the auto-enroll call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the enroll request from the client machine	1. Check whether the client certificate and key are set in the enroll certificate request. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the enrollment request.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the EST setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in the logs and failed Work order for the reason of submission failure.
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in the work order log - “Denied due to policy module”.	Check for the bit length in the CSR parameters, if it is lesser than or equal to 1024 then increase that in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling again. 2. Connect database and update the entry as given below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})" **Note:** This would allow multiple CSR’s with the same parameters in the certificate inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in obtaining CA certificate via EST

Note: From the client machine hit the get ca certificate call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the get ca request from the client machine.	1. Check whether the client certificate and key are set in the “get ca certificate request”. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a valid certificate in the **get ca cert request**.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.

Issues in auto re-enrolling certificate via EST

Note: Note: From the client machine hit the auto re-enroll call using AppViewX EST server URL which is displayed on the EST setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the EST settings.	Check for the agent IP and agent name in the client machine.
Client certificate authentication failed since no client certificate content is obtained	The client certificate is not set in the re-enroll request from the client machine	1. Check whether the client certificate and key is set in the re-enroll certificate request. 2. If the provided certificate is pfx or pkcs12 certificate check whether the provided password is correct.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Provided client certificate is not valid.	The provided client certificate might be Expired or Revoked.	Provide a Valid certificate in the re-enroll request.
HTTP authentication failed due to invalid parameters provided.	The HTTP authentication parameters provided must be invalid.	1. Check for password in BASIC authentication. 2. Check for nonce and other parameters in DIGEST parameters.
CA certificate is not found	The issuer certificate of the selected "server certificate" might have been deleted or the server certificate has been deleted.	Check for the issuer certificate and its issuer certificate available in the inventory.
Unable to establish connection with EST server.	There might be an issue with reaching the AppViewX EST agent IP from the client.	Check whether the EST agent IP is reachable from the client machine. Check whether the EST agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the EST setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check in logs and in failed Work order for the reason why submission got failed.
Unable to submit the CSR request to	There might be an error in the work order log - “**Denied due to policy module**”.	Check for the bit length in the CSR parameters, if its lesser than or equal to 1024 then increase that in the CSR.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
certificate authority - For MSCA		
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry as mentioned below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})" **Note:** This would allow multiple CSR's with the same parameters in the certificate inventory.
Enrolled Certificate is not found	While renewing the enrolled certificate, the enrolled certificate might not be present in certificate inventory.	1. Check if the enrolled cert is present in certificate inventory. 2. Check if the enrolled certificate provided in "renew request" is a valid one and is enrolled already in AppViewX. 3. If the enrolled certificate is not present in inventory, check if the authentication cert is in cert inventory.

Troubleshooting for MsIntune SCEP

Overview

This section helps you troubleshoot the common problems that you might encounter when using MSIntune SCEP functionalities like setting addition and certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in MSIntune SCEP setting addition and validating the settings

Issues in the MSIntune SCEP Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **CERT+**.
   The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **MsIntune**.
   The **Auto Enrollment MsIntune** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent ip is not reachable	The MS Intune SCEP agent IP and specified port may not be reachable from the AppViewX node.	Validate and ensure that the agent IP/Port is reachable.
Certificate does not belong to the selected CA.	The server certificate provided in the agent setting does not belong to the CA which is selected.	Please check whether the selected server certificate belongs to the CA which was selected earlier.
CA setting connection is in Failed status	The connection status of the chosen CA setting chosen in the agent setting failed.	Check the specified CA setting and make necessary changes to make it valid.

Issues in auto enrolling certificate via MS Intune SCEP

Note:

1. From the client machine, enroll for the certificate using Company Portal application.
2. Newly enrolled certificate should be available in the AppViewX CERT+ Inventory. If the new certificate is not available in the AppViewX CERT+ Inventory, even after 5 minutes from triggering the request from the device, then logon to the CLI and verify the logs for avx_vendor_cert_intune_agent plugin.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Following errors may appear in the logs:

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority	Request might have failed due to a specific error from CA	Verify the vendor logs to see if there is any CA specific error.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling. 2. Connect database and update the entry given below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"},{$set: {"constant":"no"}})" **Note:** This would allow multiple CSR's with the same parameters in the certificate inventory.
Challenge in PKCS#10 request (Transaction ID: <<transactionID>>) is not valid. Certificate enrollment will not be processed.	Challenge password validation with Microsoft Intune has failed. Possible reasons - 1. Connectivity issue with Microsoft Intune. 2. Intune credentials configured in agent settings might be incorrect.	1. Validate the internet access in the AppViewX server. 2. Check and correct the Intune Client Id/Tenant Id/Client Secret configured in the MS Intune agent setting.
No error message but enrollment request does not get triggered after	A mismatch between the CA certificate configured in the MS Intune Agent setting and	Verify and ensure that the root and intermediate CA certificates of the Server certificate available in the AppViewX MS Intune agent setting match with

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
the getCACert call from the client device.	that configured in the Intune portal.	the Root and Intermediate certificates configured in the MS Intune portal (Azure) SCEP profile.

Troubleshooting for SCEP

Overview

This section helps you troubleshoot the common problems that you might encounter when using SCEP functionalities like setting addition, enrolment, and obtaining.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported SCEP Client

• SSCEP client

• Cisco Routers

• Mobileiron Cloud portal

Issues in SCEP setting addition and check the settings

Issues in the SCEP Settings

1. Log in to **AppViewX** application with valid credentials.
2. From the left pane, expand the **menu** and click **CERT+**.
   The **Server Certificate** page is displayed.
3. From the left pane, expand **Administration**, select **Auto Enrollment**.
4. Click **SCEP**.
   The **Auto Enrollment SCEP** page is displayed.
5. Click **Add**.
6. After settings are added, click **Check** to see the validity.

Error Messages

Error Message	Possible Cause	Possible Solution
Agent name already added. Please enter a different name..	A SCEP setting with the same name already exists on SCEP Page.	Check the SCEP Setting name, it should be unique.
1. This field should not be null or empty. 2. Mandatory Field(s) - <Field name> is/are empty.	Some of the mandatory fields are missing or invalid.	Add all the valid information in the mandatory section.
SCEP setting is invalid - Agent ip is not reachable	The SCEP agent IP and port provided might not be accessible from the AppViewX node.	Please check the IP port provided so that it can be pingable from the AppViewX node.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
SCEP setting is invalid - Certificate does not belong to the selected CA.	The server certificate provided does not belong to the CA which is selected.	Please check whether the selected server certificate belongs to the CA which was selected earlier.

Issues in Auto Enrolling certificate via SCEP

Note: From the client machine hit the auto-enroll call using AppvViewX SCEP server URL which is displayed on the SCEP setting page.

Error Message	Possible Cause	Possible Solution
No agent settings found for the provided agent ip address (OR) Agent settings is not found	The provided agent IP or agent name is not found in the SCEP settings.	Check for the agent IP and agent name in the client machine.
Unable to establish connection with SCEP server.	There might be an issue with reaching the AppViewX SCEP agent IP from the client.	Check whether the SCEP agent IP is reachable from the client machine. Check whether the SCEP agent IP is open and can be accessible.
Group policy does not have the given hash function	The requested hash function in the CSR parameters may not be available in the selected policy.	1. Navigate to the policy page. 2. Select the CA used in the SCEP setting. 3. In the hash function field include the requested and missing hash functions. 4. Save the CA details and update the policy.
Unable to submit the CSR request to certificate authority	Failure due to specific CA functionality.	Check the reason for submission failure in logs and failed Work order.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to submit the CSR request to certificate authority - For MSCA	There might be an error in the work order log - “**Denied due to policy module**”.	Check for the bit length in the CSR parameters, if it's lesser than or equal to 1024 then increase it in the CSR.
CSR parameters already exists	There might be another CSR already present in the inventory for which certificates would not have been issued.	1. Delete the previous CSR present in inventory and try enrolling again. 2. Connect database and update the entry as mentioned below: "db.cert_metadata.update({"_id" : "DO_CSR_PARAMS_UNIQUENESS_CHECK"}, {$set:{"constant":"no"}})" **Note:** This would allow multiple CSR’s with the same parameters in the certificate inventory.

Issues in Obtaining CA certificate via SCEP

Troubleshooting AWS, CLOUD

This section of the guide will help you tackle the various issues that arise while using the functionalities of CLOUD services. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.AppViewX.com or send an email to help@AppViewX.com.

- Troubleshooting for AWS ACM
- Troubleshooting for AWS IAM
- Troubleshooting AWS CloudFront
- Troubleshooting AWS ELB
- Troubleshooting Azure Cloud
- Troubleshooting Cloud - Common Functionality

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting for AWS ACM

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ACM & IAM service like server addition using AppViewX, fetch, certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Server Addition using AppViewX GUI

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	Provided credential is invalid.	1. Provide valid Access Key. 2. Provide valid Secret Key.
Provide valid account name	Account name can be duplicate or not as per standard.	1. Provide unique name for account name. 2. Account name can be alphanumeric and can also have period (.) in it.
Details Incorrect	Provide mandatory fields.	Enter mandatory fields like 1. Account Number 2. Access Key 3. Secret Key 4. Data Center 5. Services 6. Regions

Issues in Fetch Regions

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	The provided credential is invalid.	1. Provide valid Access Key. 2. Provide a valid Secret key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovery in ACM

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device from which to discover certificates.

Issues in Push and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, such as in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	Userdoes not have required permissions to push to the device.	Retry after getting the access for required action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.

Troubleshooting for AWS IAM

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ACM & IAM service like server addition using AppViewX, fetch, certificate discovery & certificate push.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Server Addition using AppViewX GUI

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	Provided credential is invalid.	1. Provide valid Access Key. 2. Provide valid Secret Key.
Provide valid account name	Account name can be duplicate or not as per standard.	1. Provide unique name for account name. 2. Account name can be alphanumeric and can also have period (.) in it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Details Incorrect	Provide mandatory fields.	Enter mandatory fields like 1. Account Number 2. Access Key 3. Secret Key 4. Data Center 5. Services 6. Regions

Issues in Fetch Regions

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	The provided credential is invalid.	1. Provide valid Access Key. 2. Provide a valid Secret key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovery in IAM

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device from which to discover certificates.

Issues in Push and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, such as in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	Userdoes not have required permissions to push to the device.	Retry after getting the access for required action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.

Troubleshooting AWS CloudFront

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for CloudFront service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Issues in Discovery in CloudFront

Issues in Push-Bind and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private Key is required to push certificate to ACM inventory	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide "Modify" access for the resource and retry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.
Certificate cannot be pushed as selected Amazon CA certificate is in <SOURCE_REGION> region and region you tried is <DESTINATION_REGION>	Selected certificate is in ACM in a different region than the region to be pushed	Use certificates available in the <DESTINATION_REGION> (or) Push a new certificate to the <DESTINATION_REGION>

Troubleshooting AWS ELB

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ELB service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Device	OS	Resolution
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Discovery in ELB

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Push-Bind and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in an enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
1 validation error detected: Value at 'privateKey' failed to satisfy constraint.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because the push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to the device when certificate is unavailable, i.e, in a new state.	Push to the device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	The provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide Modify access for the resource and retry
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.

Troubleshooting Azure Cloud

This section helps you troubleshoot the common problems that you might encounter when using certificate functionalities. This guide will give more troubleshooting processes on cloud addition, deletion, push, bind, rollback, and other actions associated with Azure cloud.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7,	From AppViewX Version 11.1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
	macOS - Version 13.1.2)	
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Azure Cloud Addition using AppViewX GUI

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A Cloud Account with the same name exists in inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Azure Cloud

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Authentication to the Azure	Subscription ID, Tenant ID	Login to Azure portal and get all the valid IDs.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
cloud inventory is Failed	Client ID and Client secret of the Azure cloud account are incorrect. Check each of the provided ID is valid and active.	
Found 0 Key vault services	No Keyvault instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Keyvault instances.
Found 0 Application Gateway services	No Application Gateway instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Application Gateway instances.
Found 0 Virtual machine services	No Virtual Machine instances running for the provided Subscription ID.	Login to Azure portal and check if the Subscription ID has required permission to access the Virtual machine instances.

Issues in Accessing Azure Cloud

Access Issues might be reproduced when communicating with Azure cloud account, while discovering or fetching the services. These errors can be collected either from logs, API responses, or in the status field for that particular server.

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Connection timeout	Internet / Proxy connection is not provided from the AppViewX node. Firewall settings blocking the REST API request.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy and Check Firewall settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution

No Keyvault instances are discovered	Subscription ID doesn't have an appropriate role to access the Azure services.	Check if the following role is assigned for the provided subscription ID in Azure cloud account.
		{
		"properties": {
		"roleName": "AppViewX_KeyVault_Role",
		"description": "",
		"assignableScopes": [
		"/subscriptions/f2689969- 42f6-4fb5-b3be-e3a02e33751c"
		],
		"permissions": [
		{
		"actions": [
		"Microsoft.KeyVault/vaults/read"
		],
		"notActions": [
		],
		"dataActions": [
		"Microsoft.KeyVault/vaults/certificates/import/action",
		"Microsoft.KeyVault/vaults/certificates/create/action",
		"Microsoft.KeyVault/vaults/certificates/update/action",
		"Microsoft.KeyVault/vaults/certificates/read"
		],
		"notDataActions": [
		]
		}
		]
		}}

No Keyvault instances are discovered	Azure Keyvault doesn’t have certificate Get/List permissions in access policies.	Login to Azure portal and navigate to Azure KeyVault -> Access policies and check if the Certificate management Operations has Get and List permissions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
No Keyvault instances are discovered	Azure Keyvault Networking blocking the certificate discovery.	Login to Azure portal and navigate to Azure KeyVault -> Networking and check if the If IP is allowed to access the Keyvault in Firewalls and virtual networks.

Issues in Managed Cloud

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Cloud

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Fetch Config

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Authentication to the Azure cloud inventory is Failed	Subscription ID, Tenant ID Client ID and Client secret of the azure cloud account is incorrect.	Login to Azure portal and get all the valid IDs. Check if each of the provided ID is valid and active.

Issues in Certificate Discovery

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a devices	No cloud account is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Discovery Status Failed	Check internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
No Certificates discovered from Azure KeyVault	Keyvault instance is not discovered from Azure cloud account.	Check device status in device addition page for Azure keyvault, if we have a Keyvault instance discovered count.
No Certificates discovered from Azure KeyVault	Azure Keyvault doesn't have certificate Get/List permissions in access policies	Login to azure portal and navigate to Azure KeyVault -> Access policies and check the Certificate management Operations having Get and List permissions (refer below snapshot)
No Certificates discovered from Azure KeyVault	Azure Keyvault Networking blocking the certificate discovery	Login to Azure portal and navigate to Azure KeyVault -> Networking and check the Firewalls and virtual networks If IP is allowed to access the Keyvault. (refer below snapshot)

Issues in Certificate Import

Error messages

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages (continued)

Error Message	Possible Cause	Possible Solution
	and not completed. 3. AppConnector might not be in sync.	3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in the enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages (continued)

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate push failed. Error is, jdk.nashorn.internal.runtime.Undefined	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Certificate push failed	Check internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
{"code":"Forbidden","message":"The user, group or application 'appid=d6dde692-94d9-4a9c-8bd4-77782d22b0ef;oid=669e113f-0651-4bb5-9698-cd4e863e1ee9;numgroups=0;iss=https://sts.windows.net/e5f90d85-3cdf-457d-a611-1aca82b0843b/' does not have Certificates import permission on key vault 'keyvault-type-1;location=eastus'. For help resolving this issue, please see https://go.microsoft.com/fwlink/?linkid=2125287","innererror": {"code":"ForbiddenByPolicy"}}	Azure Keyvault instance doesn't have certificate Import permissions in access policies.	Login to Azure portal and navigate to Azure KeyVault -> Access policies and check the Certificate management Operations having Import permission.
{"code":"Forbidden","message":"Client address is not authorized and caller is not a trusted service.\r\nClient address: 125.21.72.158\r\nCaller:	Azure Keyvault Network blocking	Login to Azure portal and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages (continued)

Error Message	Possible Cause	Possible Solution
appid=d6dde692-94d9-4a9c-8bd4-77782d22b0ef;oid=669e113f-0651-4bb5-9698-cd4e863e1ee9;iss=https://sts.windows.net/e5f90d85-3cdf-457d-a611-1aca82b0843b/\r\nVault: keyvault-type-2;location=eastus","innererror":{"code":"ForbiddenByFirewall"}}	the Certificate Push.	navigate to Azure KeyVault -> Networking and check the Firewalls and virtual networks if IP is allowed to access the Keyvault.

Troubleshooting Cloud - Common Functionality

This section helps you troubleshoot the common problems that you might encounter when using cloud functionalities. This guide will give more troubleshooting processes on cloud addition, deletion, and other actions available with the cloud module.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	rom AppViewX Version 11.1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Cloud Addition using AppViewX UI - AWS

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A cloud account with the same Account name already exists in the inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.
Please provide valid credentials	The credentials provided are invalid/ has no access to fetch regions	Provide valid credentials/ credentials with needed access

Issues in Cloud Addition using AppViewX UI - Azure, GCP

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Cloud account already exists.	A cloud account with the same Account name already exists in inventory.	Check the Account name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Communicating to Cloud accounts

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Authentication to the Azure cloud inventory is Failed	Credentials provided are invalid/ credentials do not have the required access.	Validate the credentials and Check if credentials are provided required access.
Failed to communicate with GCP	Unable to connect to the endpoint.	Check if the node can reach the endpoint via proxy/internet as configured.
Failed to communicate with <SERVICE> through region <REGIONS>.	Credentials do not have required access	Provide credentials the required access

Issues in Managed Cloud Account

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	The device cannot be managed because it is already in the managed state.	Unmanage the device(s) before performing the action.

Issues in Unmanaged Cloud Account

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	The device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) before performing the action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in a managed state.	Manage the device(s) in an unmanaged/in-progress state before performing an action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issue in Discovery

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. The Discovery name is not given or the length is less than 2 characters. 2. The interval between batches info is missing when the execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates.

Troubleshooting Server, Firewalls, WAF, and Rapid SB Connectors

This section of the guide will help you tackle the issues encountered while using the functionalities of servers, firewalls, WAF, and Rapid SB Connectors. It deals with common functionalities of these devices at the beginning of each guide and the rest of the guide deals with functionalities of specific devices. If the problem still remains unresolved please send a request to Technical Support by opening a case with the AppViewX Technical Services team. You can open a case from helpcenter.AppViewX.com or send an email to help@AppViewX.com.

- Troubleshooting Apache Linux
- Troubleshooting Barracuda WAF
- Troubleshooting Cisco ASA Firewall
- Troubleshooting Cisco CallManager
- Troubleshooting Common Functionality of Servers
- Troubleshooting Data Power Server
- Troubleshooting F5 WAF
- Troubleshooting Fortigate Firewall
- Troubleshooting HP ILO
- Troubleshooting IBMClient Linux
- Troubleshooting IBMClient Windows
- Troubleshooting Imperva WAF

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Troubleshooting Linux JBoss Server
• Troubleshooting for Microsoft Enterprise CA Issues
• Troubleshooting Microsoft Tomcat
• Troubleshooting MQServer Linux
• Troubleshooting MQServer Windows
• Troubleshooting MS SQL Windows
• Troubleshooting Nginx Server
• Troubleshooting NginxPlus ADC
• Troubleshooting Paloalto Firewall
• Troubleshooting Panorama Firewall
• Troubleshooting Check point Firewall
• Troubleshooting RabbitMQ Server
• Troubleshooting Rapid SB Server Inventory
• Troubleshooting Rapid SB Linux Server
• Troubleshooting Tomcat Linux
• Troubleshooting Weblogic Linux
• Troubleshooting Websphere Linux
• Troubleshooting Websphere Windows
• Troubleshooting Windows Apache Server
• Troubleshooting Windows JBoss Server
• Troubleshooting Windows Weblogic Server

Troubleshooting Apache Linux

This document helps you troubleshoot the common problems that you might encounter when using Apache Linux functionalities. This guide will give more troubleshooting processes on issues related to Apache Linux server. The issues are device addition, communication to the server, CSR generation, access to server, fetch configuration, discovery along with push and rollback.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating with the Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device ip/fqdn as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Ip is not reachable/invalid.	Invalid credentials	Kindly check the credentials provided.
	IP is not reachable	Kindly check if IP is pingable or not and make it up and running.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	IP is blocked by the firewall	Kindly check firewall settings.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Communication Failed	Username or password may be invalid	Check and provide the correct username and password.
java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods.	Authentication Failure	Provide correct credentials for authentication. Make sure SSH is enabled on the given server.
Linux rest agent communication failed.	Rest agent running on the destination machine might be down.	Please check the status of the rest agent in the destination machine.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Access

Access Issues occur while communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	File might not be present in the avx environment.	Check whether someone deleted the file from AppViewX environment.
	user might not have permission to read in the given source location.	Verify if read permission is given for the location.
	Device communication might not be established when service has started.	Verify the device connection and restart the service.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Parsing apache configuration failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
	AppViewX is not able to read/ parse the Config files from the server.	Check if the server has proper config files related to Apache Server and AppViewX has proper read permissions.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Barracuda WAF

This section helps you deal with the various issues faced by you during the use of Barracuda WAF functionalities.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Device communication failed	1. The given credential is incorrect. 2. The given IP/FQDN and Port may be incorrect. 3. Device not reachable.	1. Check and input the correct credential. 2. Check and input the correct IP/FQDN and Port. 3. Ensure the device is up and accessible.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible. 2. No valid certificates available.	1. Ensure target device is up and running. 2. Check the device has valid certificate files.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Push failed due to invalid certificate	Push failed when pushing a certificate without key.	Ensure the certificate matches with the key associated in the device on pushing without the key file.
Device is not in managed state	Device is not available in “managed list”.	Please check the device status in device inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Cisco ASA Firewall

This section will guide you to overcome the various issues faced by you during the use of Firewall Cisco ASA and its various functionalities.

Issues in Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	Interfaces are not associated with any trustpoints.	Kindly ensure the interfaces are bounded with required trustpoints. Command to verify SSL-config: show running-config SSL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Certificate push failed due to Unsupported bit length.Please provide valid one.	Unsupported bit length.	Kindly ensure the bit length of certificate is supported by ciscoASA
Cert push got failed due to ERROR: Import PKCS12 operation failed	Issues in creating trustpoints	Kindly ensure that the trust points get created successfully.

Issues in Certificate Bind

Error Message	Possible Cause	Possible Solution
Certificate bind failed due to invalid interface name or error while communicating with device.	Invalid trustpoint.	Kindly ensure the trustpoint is available on the device.

Troubleshooting Cisco CallManager

This section will guide you to overcome the various issues faced by you during the use of Cisco CallManager and its various functionalities.

Issues in Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A Cisco CallManager device exists in inventory with the same name.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <hostname name> has failed.	1. Device unreachable. 2. Invalid credential. 3. Invalid port.	1. Kindly check if the given IP/FQDN is reachable. 2. Kindly check the credentials provided. 3. Kindly check the port and firewall settings.
Cisco Tomcat service is not active	Cisco Tomcat service is not in an up and running state.	Kindly restart the Cisco Tomcat Service. Command to verify the status of services is: utils service list

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	Required Services may not be in an up and running state.	Please ensure the supported services are up and running state and services are associated with SSL configs. Services supported by AppViewX : Cisco tomcat Command to verify the status of services is: utils service list

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CUCM CSR gen command failed	Command execution may fail.	Kindly ensure all CSR gen commands are executed properly.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Cert push got failed due to Error while importing server certificate.	1. The certificate should be issued from CSR generated by device. 2. CUCM will not allow to push the same cert again.	1. Kindly ensure the certificate issued by the CSR generated from Device.CUCM will not support to push any other certs. 2. CUCM will delete the CSR information from the device on successful cert push. Kindly ensure you are pushing the newly issued certificate and respective CSR information for the same should be available in the device.
Cert push got failed due to Error while importing trust certificate.	CA/Intermediate cert with the same name may already exist in the device.	AppViewX will not overwrite the existing CA configurations. Kindly delete/rename the old certificates to proceed with push.

Issues in Certificate Bind

Error Message	Possible Cause	Possible Solution
Cert bind got failed.Cause : Service restart failure.	Connection timeout or Invalid Services	Kindly check if the device is in a reachable state to execute the command.

Troubleshooting Common Functionality of Servers

This section helps you troubleshoot the common problems that you might encounter when dealing with the common functionality of servers. The guide will give more troubleshooting processes on issues encountered during handling of devices like addition using import option, adding to credential list, including the server in managed servers, unmanaging the server or server export.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device Addition using Import Option

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are csv/xls/xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In the file history of the import page maximum 5 files can be maintained.	Delete any of the parsed/completed files to upload a new one.

Issues in Credential List Addition

Issues in the Server Unmanage Functionality

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in the Server Manage functionality

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Server Export

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue.	Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.)
	Unable to fetch device list from the database.	Make sure the database is running and has correct data.

Troubleshooting Data Power Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with the Data Power server.

Issues in Data Power Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Data power Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Domain fetch has failed.	Domain not configured in Data Power	Check manually if domains are configured.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching domains. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Rest communication failed	Unable to access the Rest APIs exposed by Data Power	Login via Postman to check if the APIs are accessible

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “**Discover By**” section.	Select at least one device to discover certificates from.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the store to push the certificate in the application connector	Kindly ensure the user has access to the store to push the certificates to.

Troubleshooting F5 WAF

This section helps you troubleshoot the common problems that you might encounter when using the F5 WAF functionalities. This guide will give more troubleshooting processes on F5 WAF certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with F5 WAF.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the associated error message.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the error message associated.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
CSR Generation using HSM on this device version is not supported.	Version not supported.	Please use the supported version device to create CSR using HSM. Supported versions are v13 and v12.
1) CSR content unavailable in device 2) Requested CSR is not available in device 3) Csr could not be fetched	CSR content unavailable on device.	For some reasons CSR creation has failed, please check the logs to reproduce.
CSR already exists in this scope with the same Key reference name	The name is already used on the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Thales HSM is not installed in the device. Please install and try again.	Thales is not installed in the device.	Please install Thales HSM and try again.
Invalid module. Please specify the valid module and try again.	Invalid module specified.	Specify a valid module and try again.
The CSR <name> was not found in the device.	CSR content is not available in the name specified.	Please check the name in the CA connector.
NetHSM private key is not available/installed in device	NetHSM private key is not available/installed in the device.	Please install NetHSM private key on the device.

Issues in F5 WAF Backup, Push, Bind, and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
Invalid profile type	Specified profile type is not supported.	Please use client-SSL or server-SSL.
Certificate fetch failed	Certificate fetch failed.	Check the error message associated to know more about the problem.
Certificate already exists	Certificate is already available with the same.	Either change the name or enable overwrite in the application connector.
Key already exists	Key is already available with the same.	Either change the name of the key or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates only can be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Fortigate Firewall

This section helps you troubleshoot the common problems that you might encounter when using the Fortigate firewall in CERT+ functionalities. This guide will give more troubleshooting processes on Fortigate firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Fortigate firewall.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Error occurred in command execution - <Error message>	Error occurred in command execution	Command execution has failed. Please refer to the error message associated with this.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.
Error occurred in command execution - <Error message>	Error occurred in command execution.	Command execution has failed. Please refer to the associated error message.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Csr name exists in the device, and cannot be overwritten.	Name is already used in the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.

Issues in Fortigate Firewall Backup, Push, Bind and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate content is mandatory parameter	Certificate content should be available.	Please specify certificate content in the request.
Intermed certificate content is mandatory for pushing CA certificate	Intermediate certificate content should be available.	Please specify intermediate certificate content in the request.
Root certificate content is mandatory for pushing CA certificate	Root certificate content should be available.	Please specify root certificate content in the request.
Certificate name is mandatory parameter	Certificate file name is mandatory.	Please specify the certificate file name in the connector.
Profile details are missing in Application connector	Profile details are missing.	Please specify profile details in the request.
Private key password is mandatory parameter	Private key password is mandatory.	Specify private key password in the connector.
Given certificate name does not exist in a device with a private key. Certificate with private key should exist either in device or AppViewX	Private key not available in the certificate.	Certificate should be pushed with the private key to bind with the profile.
Root certificate name already exists in ca store, Cannot overwrite until Overwrite is enabled in Connector	Overwrite is not enabled in the application connector.	Enable overwrite option in the application connector.
Intermediate certificate with name: <name> already exists in ca store, Cannot overwrite until Overwrite is enabled in Connector	Overwrite is not enabled in the application connector.	Enable overwrite option in the application connector.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates can be pushed.

Troubleshooting HP ILO

This section will guide you to overcome the various issues faced by you during the use of HP ILO and its various functionalities.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <ip/ fqdn> has failed.	IP/FQDN provided is not reachable. Credentials not valid.	Check if the provided IP/FQDN is correct Check if the provided username and password for device addition is correct The HPILO python package is not installed properly in AppViewX VM.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	ILO portal is not up and running Network issues in reaching the portal	Kindly ensure the ILO web portal is up and running. Kindly ensure a proper identity certificate is associated with the web portal

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution

CSR generation failed.
 	
`03/01/2021 20:59:45 - CSR creation in device failed due to File /tmp/certconnectors/script_16197_287072988142466.py, line 1, in <module>`
 	
`import hpilo;ilo = hpilo.Ilo('ilo.AppViewX.net', 'administrator', '19160456');print (ilo.certificate_signing_request(common_name='mtestilo1'));`
 	
IloGeneratingCSR: The iLO subsystem is currently generating a Certificate Signing Request(CSR), run script after 10 minutes or more to receive the CSR.
 	
03/01/2021 20:59:45 - CSR Submission Failed
	1. Input parameters might not be valid for the CSR request.
	2. Multiple CSR requests might be triggered within a short span of time.
		Kindly ensure the CSR parameters are configured properly.
		
		Kindly ensure multiple CSR requests are not submitted to the same device in any mode.
		
		Kindly ensure we keep at least 15mins interval between CSR request submission else the response for the previous request is triggered before submitting the next request.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution

Certificate Push failed
 	
`03/02/2021 10:39:49 - ILO cert push failed due to File /tmp/certconnectors/script_87672_336277286169629.py, line 1, in <module>`
 	
`--> 1 import hpilo;ilo = hpilo.Ilo('ilo.AppViewX.net', 'administrator', '19160456');print (ilo.import_certificate('''-----BEGIN CERTIFICATE-----`
 	
IloError: Invalid certificate common name
	Certificate is not generated with CSR from device	Kindly ensure the certificate is signed with a CSR request generated from the target device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
03/02/2021 10:39:49 - Push Task Failed		

Troubleshooting IBMClient Linux

This section will guide you to overcome the various issues faced by you during the use of IBMClient Linux and its various functionalities.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent GSKit is not installed on any given device.	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent. Please ensure GSKit is installed properly.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid KDB/keystore files available in the given path.	Ensure the given certificate location has a valid KDB/keystore and KDB/keystore has certs.
Discovery completed successfully. (with 0 certs even if valid certs exist in given path)	1. Respective Keystores password is not added in Password Vault to parse certs. 2. User may not have read permission to parse certs	1. Please enter the password of keystores in the Password Vault to parse certs. 2. Please ensure the user has appropriate permission to read files.

Issues in CSR Generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Certificate Push failed. Or Push got failed due to User has no permission for the given location to perform the operation	User has restricted access to the path configured to push the certificate in the application connector	Please ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available on device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device.	Ensure the target KDB file, for which certificate push configured is available and has read/write access.
1. Private key should not be empty/null. 2. Push failed due to Failure while importing certificate into keystore due to either wrong password or tampered keystore.	Trying to push certs without a keyfile.	Please ensure the certificate to be pushed has a private key file. Or if key file exists in device please select privateKeyInDevice option.

Troubleshooting IBMClient Windows

This document will guide you to overcome the various issues faced by you during the use of IBMClient Windows and its various functionalities.

Issues in Server Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable.	Ensure gateway is configured properly and the APIs are accessible from AppViewX.
	Device not reachable from the gateway agent	Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	GSKit is not installed on any given device.	Please ensure GSKit is installed properly.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid KDB/keystore files available in the given path.	Ensure the given certificate location has a valid KDB/keystore and KDB/keystore has certs.
Discovery completed successfully. (with 0 certs even if valid certs exist in given path)	1. Respective Keystores password is not added in Password Vault to parse certs. 2. User may not have read permission to parse certs	1. Please enter the password of keystores in the Password Vault to parse certs. 2. Please ensure the user has appropriate permission to read files.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
1. Failure response obtained on consuming REST API. 2. CSR submission failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
1. Push Failed. CTGSK3026W The key file "D:/mtest/mtest.kdb" does not exist or cannot be read. 2. Push got failed due to Windows Gateway Error Response : a693c520-940d-478a-8aed-7c06c3a707c2: No path found	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Push Failed due to KDB push failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.
Private key is not available. Failing the push	Trying to push certificates without a keyfile.	Please ensure the certificate to be pushed has a private key file Or if key file exists in device please select privateKeyInDevice option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Imperva WAF

This section will guide you to overcome the various issues faced by you during the use of Imperva WAF and its various functionalities.

Issues in Communicating to Imperva

Error Message	Possible Cause	Possible Solution
Communication to <ip> has failed	Invalid credentials Imperva WAF is down.	Please check if the correct Imperva credentials are provided. Please login to the SecureSphere console to check if Imperva is running.
Connection timeout	Internet / Proxy connection is not provided from AppViewX node. Firewall settings blocking the REST API request	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy and Check Firewall settings

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <ip> has failed	Invalid credentials Imperva WAF is down.	Please check if a correct Imperva credentials are provided Please login to the SecureSphere to check if Imperva is running.
Device has 0 sites.	No sites configured in Imperva.	Please login to the SecureSphere to check if Sites are configured.
Device has 0 Server Group	No Server Groups configured in Imperva.	Please login to the SecureSphere to check if Server Groups are configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device has 0 Services	No Services configured in Imperva	Please login to the SecureSphere to check if Services are configured.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a devices	No WAF account is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Discovery Status Failed	Check if internet /Proxy connection is provided in AppViewX node.	Login to AppViewX portal and provide proxy details in Menu->Settings->General->Proxy.
No Certificates discovered from Imperva WAF	SSL Certificates are not discovered from Imperva due to API restrictions. Imperva Rest API doesn't allow the public Certificate String in the API responses. Only Certificate attributes like common name, signature, Expiry date and Issuer details are captured.	Check with AppViewX PM team / SME for more details

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issue in Push and Rollback

Error Message	Possible Cause	Possible Solution
An item with this name already exists - please select a different name	SSLKeyName should be unique.	Kindly ensure to provide a unique name in “Certificate File Name” field on Connector page.
Site not found	Unable to find the site to push the certificate	Please login to SecureSphere to check if the Site is available.
Server Group not found	Unable to find the Server Group to push the certificate	Please login to SecureSphere to check if the Server Group is available.
Services not found	Unable to find the Service to push the certificate	Please login to SecureSphere to check if the Service is available.

Troubleshooting Linux JBoss Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities.This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux JBoss server.

Issues in Linux JBoss Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Communicating to Linux JBoss Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is either null or empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed.	Problem with port configuration	Check if the configured port in the device addition page is correct.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings		
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMACs configured in the target device and ensure AppViewX SSH-plugin supports the same
<IP/FQDN> has 0 JBoss instance(s)	No JBoss server running in the target device,	Login via SSH to the target device and execute the below command to check the status of the JBoss server “ps -ef | grep jboss”.

Issues in Accessing the Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Permission denied for file/ location.	File might not be present in the avx environment. User might not have permission to read in the given source location. Device communication might not be established when service has started.	Check whether someone deleted the file from AppViewX environment. Verify if read permission is given for the location. Verify the device connection and restart the service.

Issues in Credential List

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Issues in Managed Server

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Unmanaged Server

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are CSV/Xls/xlsx only. Check for the extension of the uploaded file.
Maximum five files allowed, please delete any completed file.	Maximum of 5 files can be maintained in file history of import page.	Delete any of the parsed/completed files to upload a new one.

Issues in Export Server

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue.	Provide access to be able to create the file on the local system. (e.g. check the directory where it is trying to export and give access to AppViewX for that directory)
	Unable to fetch device list from the database.	Make sure the database is running and has correct data.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	Verify the input details and check device status error messages in the Issues in Communicating to Linux JBoss Server section.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have the required permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct “connectorId” if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available in device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR generate option from Device.

Troubleshooting for Microsoft Enterprise CA Issues

This section helps you troubleshoot the common problems that you might encounter when using functionalities like setting addition, certificate enrollment, renewal, revocation, suspension, reinstation, discovery, and other actions associated with Microsoft Enterprise.

Issues in Configuring Microsoft Enterprise CA and Fetch CAs

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to save CA settings CA Settings name already exists.	A CA setting with the same name for Microsoft Enterprise already	Check the CA Setting name, it should be unique.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	exists in inventory.	
• **This field should not be null or empty** • **Mandatory Field(s) - <Field name> is/are empty** • **CA Settings - [<Fields>] mandatory fields cannot be empty.**	Some of the mandatory fields might be missing or invalid.	Add all the valid information in the mandatory section.
Unable to establish connection with CA	The configured CA details may be incorrect.	Check the CA details configured on the CA settings page.
	Proxy details may not be configured.	heck whether proxy details are configured in proxy settings.
	AppViewX may not be able to reach CA.	Check whether network access is available.
767cf2b6-bfc3-45a0-9490-a95cf841e693: Connecting to remote server <SERVER> failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: The computer <SERVER> is unknown to Kerberos. Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. The most common Kerberos configuration issue is that an SPN with the	Kerberos configuration is not configured for the target machine. The most common Kerberos configuration issue is that an SPN with	The issue occurs with Powershell Remoting since it uses Kerberos Authentication. • In Agent Machine start command prompt as Administrator and execute the following command • setspn –s http/machinename domain\username. • Please note this will work in environments where Kerberos

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
format HTTP/<SERVER> is not configured for the target. If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic	the format HTTP/ <SERVER> is not configured for the target.	Authentication is set up and there is an AD Domain Setup • If no kerberos authentication is set up then we need to communicate via WMI. • Verify that the computer exists on the network, that the name provided is spelled correctly, and that the Kerberos configuration for accessing the computer is correct. • If Kerberos is not required, specify the Negotiate authentication mechanism and resubmit the operation. For more information, see the about_Remote_Troubleshooting Help topic.
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) **OR** **Error Code 0x80070005 - Access is denied**	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group.
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "`Enable-PSRemoting -force`". 4. Execute "`netsh winhttp show proxy`" and if a proxy is configured then we need to reset it via "netsh winhttp reset proxy". 5. For more information, see the about_Remote_Troubleshooting Help topic.
41783361-015b-453f-b321-e31709b1850c: Connecting to remote server <SERVER> failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.	Access is denied.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		• Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig". • Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
The client cannot connect to the destination specified in the request. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Verify that the service on the destination is running and is accepting requests. 5. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. 6. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
d4f98a6a-41ef-4864-9848-03a07e113d75: CCertRequest::Submit: The RPC server is unavailable. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)	The Remote Procedure Call Service is not responding.	Navigate to the target machine and start RPC service if it has stopped.
727838ed-151e-46bf-883c-07ccb3a3989f: Connecting to remote server ptpld005 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group. • Check if WinRM service is running. • Navigate to Powershell on the target machine and run "WinRM QuickConfig".

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		• Execute "Enable-PSRemoting -force". • For more information, see the about_Remote_Troubleshooting Help topic.
fd3812f9-030a-421c-81e7-0e0510ce49e0: Access to the path <PATH> is denied.	The username or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group. • Navigate to Local Users and Groups and access "Administrators". Check if the configured username is part of the administrator group.
This site can’t be reached	This site can’t be reached.	• Windows Gateway is not reachable from AppViewX. • Windows Gateway service is down.
Html response : Access is denied	Access is denied.	• In Target machine's Local Computer certificate store, Trusted Root Certification Authorities should have Root CA certificates and Intermediate Certification Authorities should

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		have intermediate certificates only. • Client certificate used in AppViewX is not imported in Target machine's Local computer store.

More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator
		1. Check existing config winrm get winrm/config.
		2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring
		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		.

Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. **This user is allowed a maximum number of 4 concurrent shells, which has been exceeded.**	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config winrm get winrm/config. 2. Change the settings to increase the maxshellsperUser to 100 on the Remote machine wherein this issue is occurring

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution

Close existing shells or raise the quota for this user.		`winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}'`
		
		`winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}'`
		
		`winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'`
		
		.

Client Certificate gives Permission Denied 403 error. **This can happen in certain environment and its intermittent**	CA Store mismatch or invalid client certificate used.	Check if the Client certificate is installed correctly by checking the chain in the Personal Store. • Root of the client certificate should be available in the Trusted Root Certification Store of the Server. • Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. • If all the above looks good then go to the agent server and do the following steps 1. MMC. 2. Add “Add/Remove SnapIn. 3. select certificates. 4. select “LocalMachine”. 5. Navigate to the Personal Store and click on the client certificate. 6. Navigate to Chain.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		7. Export the Root certificate and save it as Root.cer in a location. 8. Import the “Root.cer” into trusted Root back again. 9. If the issue still remains unsolved, then check if the Trusted root contains and non-root certificates. 10. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. 11. Take a backup of such certificates and move it to respective stores. 12. If the issue remains unsolved, then add the root certificate to "Client Certificate Issuers".
The permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
803f4314-3a11-486a-87e5-367b8c5c6f9f: The user name or password is incorrect.\r\n	The user name or password is incorrect.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group
42abe1ef-2bff-40e8-82e2-c97c5707a0c1: Connecting to remote server avxstca failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	The user name or password is incorrect.	Check if the credentials are valid.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.	Powershell remoting is not configured.	1. C:\Windows\system32>WinRM quickconfig 2. WinRM service is already running on this machine. 3. WinRM is not set up to allow remote access to this machine for management. 4. The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		• Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
• **There is not enough space on the disk** • **The WSMan service could not launch a host process to process the given request. Make sure the WSMan provider host server and proxy are properly registered. For more information, see the about_Remote_Troubleshooting Help topic.** • **Execute process failed Machinename mspwvadsnybcc01.csc.nycnet, ProcessName Powershell -NoProfile - ExecutionPolicy Bypass -Command C:\\Windows\\Temp\ \1jmtip3g.sjl\1jmtip3g.sjl.ps1, Error is, Stack trace Management Cannect to remote machine mspwvadsnybcc01.csc.nycnet as user failed with the following error Value does not fail within the expected range.**	There is not enough space on the disk.	Ensure that your hard disk has enough free space.
Management Connect to remote machine VMEUSWPCA021.us.int.safelite.net as user failed with the following error User credentials cannot be used for local connections	User credentials cannot be used for local connections.	• The username should be configured as "Username@Domain". • The user should have admin access to the Remote machine (Target Machine) or should be part of the Local Administrator group. • Navigate to Local Users and Groups and access

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group. • or configure the credentials in AppViewX.CertPlus.Service Logon option.
Device Communication failed while using Native option to connect to CA remotely	Local System Account doesn't have access to CA. Please change the logon credentials in service.	1. Navigate to agent machine.. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find the service "AppViewXCertPlus". 4. Right-click and view properties. 5. Click "log on" tab. 6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a message will pop up to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service 9. Remove the username and password from AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Enrolling, Renewing, and Regenerating a Microsoft Enterprise CA Certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	Check the CA details configured on the CA settings page. Check whether proxy details are configured in proxy settings. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.
The account configured in Application pool identity don't have access to the requested Template	User doesn’t have access	Please give access to the user.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	to the template.	
DATA is invalid log message	Invalid header for CSR.	Replace (----BEGIN NEW CERTIFICATE REQUEST----) with (----BEGIN CERTIFICATE REQUEST----) and Replace (----END NEW CERTIFICATE REQUEST----) with (----END CERTIFICATE REQUEST----)
Error Code 0x80070005 - Access is denied	Access not available.	1. Agent and CA Should be under the same domain. 2. ApplicationPoolIdentity of IIS Agent site should be a Custom account with admin credentials. 3. To verify template name, Go to CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it, and select properties, In General Tab, you can find Template name which needs to be used in AppViewX. 4. To check Template permission, Go to the CA portal, Right. Click on Certificate templates, Select Manage, Select the template, right-click on it and select

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		properties, in the security tab check all permissions given for the user.
Retrieving the COM class factory for remote component with CLSID	Unable to connect to certificate authority.	1. The Component used for accessing CA (certadm.dll) is not installed or has permission issues. 2. Check if dll is available in C:\Windows\System32 folder else install Microsoft Remote Server Administration Tools (RSAT) for the respective OS. EX: for Windows 10 https://www.microsoft.com/en-in/download/details.aspx?id=45520
PowerShell ScriptExecution Error: Access is denied. 0x80070005 (WIN32: 5) OR Error Code 0x80070005 - Access is denied	Access is denied.	1. The username should be configured as "Username@Domain". 2. The user should have admin access to the Remote machine (Target Machine) or should be part of Local Administrator group 3. Navigate to Local Users and Groups and access

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		"Administrators". Check if the configured username is part of the administrator group.
the permission on the certificate template do not allow the current user to enroll for this type of certificate	User does not have access to the certificate template used for enrollment.	1. Navigate to CA Server. 2. Open Certificate Authority. 3. Select the CA Server. 4. Right-click on properties. 5. Click on Security Tab. 6. Check if the user used in Agent has the necessary permissions to read, issue and manage certificates and request certificates. 7. If a user is part of a group then please ensure that the group has permissions. 8. Click on Certificate Templates and right-click to manage templates. 9. Right-click on the template which has the issue and navigate to security. 10. Add permission to the user or group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
An attempt was made to open a Certification Authority database session, but there are already too many active sessions" on a request using CERTADMINLib.IenumCERTVIEWROW.Next().	The Certification Authority database has too many active sessions.	In CA server navigate to registry via regedit command and set the following: 1. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBSessionCount` to 64 hex (100 Dec). 2. `HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBMaxReadSessionCount` is also set to 64 hex (100 Dec).
The WinRM client received an HTTP status code of 502 from the remote WS-Management service. For more information, see the about_Remote_Troubleshooting Help topic	Powershell remoting not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force". 4. Execute "netsh winhttp show proxy" and if a proxy is

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		configured then we need to reset it via "netsh winhttp reset proxy".
The client cannot connect to the destination specified in the request. Verify that the service on the dest ination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running o n the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"	Powershell remoting is not configured.	1. Check if WinRM service is running. 2. Navigate to Powershell on the target machine and run "WinRM QuickConfig". 3. Execute "Enable-PSRemoting -force".
More than 5 connections are not allowed	Powershell configuration has restricted access for concurrent script executions.	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Connecting to the remote server failed with the following error message : The WS-Management service cannot process the request. This user is allowed a maximum number of 4 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.	Powershell configuration has restricted access for concurrent script executions	Run Powershell as Administrator 1. Check existing config 2. winrm get winrm/config. 3. Change the settings to increase the maxshellsperUser to 100 on

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		the Remote machine wherein this issue is occurring: • `winrm set winrm/config/winrs '@{MaxConcurrentUsers="20"}` • `'winrm set winrm/config/winrs '@{MaxShellsPerUser="100"}` • `'winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'.`
Client Certificate gives Permission Denied 403 error. This can happen in certain environment and its intermittent	1. Certificate store mismatch. 2. Invalid client certificate specified.	1. Check if the Client certificate is installed correctly by checking the chain in the Personal Store. 2. Root of the client certificate should be available in the Trusted Root Certification Store of the Server. 3. Intermediate of the client certificate can be available in the Intermediate Certification authorities of the Server. 4. If all the above looks good then go to the agent server and do the following steps: a. MMC. b. Add “Add/Remove SnapIn. c. select certificates. d. select “LocalMachine”. e. Navigate to the Personal Store and click on the client certificate. f. Navigate to Chain.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		g. Export the Root certificate and save it as Root.cer in a location. h. Import the “Root.cer” into trusted Root back again. i. If this also doesn’t solve the issue then check if the Trusted root contains and non-root certificates. j. Click on the “Trusted Root” store and check if there are certificates that have different IssuedTo and IssuedBy. k. Take a backup of such certificates and move it to respective stores. l. Even after this if it doesn't solve then add the root certificate to "Client Certificate Issuers".
Certificate Request (CSR) is using different account to request certificate from CA as compared to account configured in AppViewX		1. Navigate to the agent machine. 2. Open services.msc using Start>>Run command on the windows machine. 3. Find service "AppViewXCertPlus" 4. Right-click and view properties. 5. Click on "log on" tab

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		6. Change the option to this account and enter the user account and password information. 7. Click on "Apply" and a popup message will appear and ask you to add an account as "Log on as service". Click "OK" and save the changes. 8. Click on restart the service. 9. Remove the username and password from AppViewX.
CSR Parameters invalid error	CSR Parameters supplied mismatch with Selected template/CA's Policy.	Supply valid CSR values accepted by template or CA policy.
Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: WebServer1.	Incorrect certificate template used.	Use template name instead of the template display name.
Connecting to remote server ptpld334 failed with the following error message : WinRM cannot complete the operation. Verify that the specified computer name is valid, that the computer is accessible over the network, and that a firewall exception for the WinRM service is enabled and allows access from this computer. By default, the WinRM firewall exception for public profiles limits access to remote computers within the	Powershell remoting is not configured.	C:\Windows\system32>WinRM quickconfig WinRM service is already running on this machine. WinRM is not set up to allow remote access to this machine for management.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
same local subnet. For more information, see the about_Remote_Troubleshooting Help topic.		The following changes must be made: • Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine. • Make these changes [y/n]? y • WinRM has been updated for remote management. • Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Revoking Microsoft Enterprise certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for revocation	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Suspending Microsoft Enterprise certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for suspension.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Reinstating Microsoft Enterprise certificate

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Invalid reason specified.	Invalid reason specified for reinstatement.	Please use the correct reason supported by the CA.
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured in the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovering Microsoft Enterprise certificates

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to establish connection with CA	1. The configured CA details may be incorrect. 2. Proxy details may not be configured. 3. AppViewX may not be able to reach CA.	1. Check the CA details configured on the CA settings page. 2. Check whether proxy details are configured in proxy settings. 3. Check whether network access is available.
Empty response received from windows gateway.	1. CA certificate stores may have mixed type certificates. 2. Client certificate may be wrong.	1. Enable custom client authentication or Check Local Machine's Root certificate store should have Root certificates only and Intermediate certificate store should have Intermediate certificates only. 2. Check whether the client certificate is valid.

Troubleshooting Microsoft Tomcat

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Microsoft Tomcat server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Microsoft Tomcat Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Tomcat Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct details and click Save.
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Parsing for PTPLD178 completed. 0 ports parsed.	Invalid Tomcat	Login manually into the windows server and find the Tomcat

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Server path	installation directory path and provide the same path in Server path attribute of tomcat device addition page
Error on fetching Tomcat instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location 3.Device communication might not be established when service has started.	1.Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3.Verify the device connection and restart the service.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username /	Verify the input details and check for device status error messages in the Issues in Communicating to Tomcat Server section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Password of the device added might be wrong.	

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e. in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/ write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	"Private key in Device" is enabled in application connector and also private key is available in the certificate	Ensure "Private key in Device" attribute in application connector is unchecked.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available in device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting MQServer Linux

This section will guide you to overcome the various issues faced by you during the use of MQServer Linux and its various functionalities.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added could be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration	Check if the configured port in the device addition page is correct.
Device communication (02/24/2021 05:07:25 PM) Failure	MQ is not configured in the target device	Check if MQ server is configured in the target device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Communication to 192.168.133.31 has failed Device Version (02/24/2021 05:07:25 PM) Failure Device version fetch has failed		Check MQ toolkit is installed in the target device
Device communication (02/24/2021 06:12:50 PM) Failure Communication to 192.168.133.30 has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMacs configured in the target device and ensure AppViewX SSH-plugin supports the same

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	MQServer QManager is not up and running.	1. Login to the target device 2. Switch to user which has mqm group access 3. start the QManager Command: `strmqm <qname>`
Received failed response from batch	No valid KDB files available in the path configured to the QManager	Ensure the path configured in QManager has valid KDB files and KDB has certs. Command to find path:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		`echo "DIS QMGR SSLKEYR" | runmqsc`

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.

Troubleshooting MQServer Windows

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with MQServer Windows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <hostname> failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> failed Device version fetch has failed.	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	MQServer QManager is not up and running.	1. Login to the target device 2. Switch to user which has mqm group access 3. start the QManager Command: strmqm <qname>
Received failed response from batch	No valid KDB files available in the path configured to the QManager	Ensure the path configured in QManager has valid KDB files and KDB has certs. Command to find path: echo "DIS QMGR SSLKEYR" | runmqsc.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
Failure response obtained on consuming REST API. CSR submission failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Push Failed. CTGSK3026W The key file "D:/mtest/mtest.kdb" does not exist or cannot be read.	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Push Failed due to KDB push got failed.	Target KDB file does not exist in the device	Ensure the target KDB file, for which certificate push configured is available and has read/write access.

Troubleshooting MS SQL Windows

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback and other actions associated with MS SQL Windows.

Issues in Communicating to MS SQL

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable.	Ensure gateway is configured properly and the APIs are accessible from AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Device not reachable from the gateway agent	Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> has failed	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.
Device version fetch has failed.	MSSQLSERVER service instance is down	Restart the MSSQLSERVER instance
Device version fetch has failed.	Command not supported by MS SQL version	Execute the version command SQLCMD -Q 'SELECT @@VERSION;' -t 3 in the CLI of the device to check if it returns version response

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
PTPLD178 has 0 instances.	No installed MS SQL instances. Installed instances are not up and running.	Execute (get-itemproperty 'HKLM:\\SOFTWARE\\Microsoft\ \Microsoft SQL Server').InstalledInstances in the device as a powershell script and check if it returns the MS SQL instances

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issue in Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid certificates in store that are binded to the MS SQL instances.	Ensure the certificates are binded to a MS SQL instance.

Issue in CSR generation

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issue in Push and Rollback

Error Message	Possible Cause	Possible Solution
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key.If privatekey is available in device please select privateKeyInDevice option.
Error: “/LOCAL_MACHINE/ CertificateAuthority” does not exist	CertificateAuthority Store is removed from the Store	Create a CertificateAuthority store.

Troubleshooting Nginx Server

This section helps you troubleshoot the common problems that you might encounter when using certificate Nginx Server functionalities.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Communication to <IP> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	1. Given credentials	1. Check and input

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	are incorrect. 2. Given IP may be incorrect. 3. Device not reachable	the correct credential. 2. Check and input the correct IP 3. Ensure device is up and accessible

Issues in Certificate Directory

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	1.Kindly ensure the user configured for device addition has read/write access to the path configured. 2. For sudo user, Please check the access elevation configured in device addition

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Failure during push operation to the server Nginx due to Private key should not be empty or null.Please provide valid key to proceed push.	Private key not available in push request certificate	Please ensure the private key is available in request
Pivatekey In device configured. But key content is available with the certificate from AppViewX.. So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Privatekey not exists in device.	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting NginxPlus ADC

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with NginxPlus ADC.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Private key should not be empty or null.	Private key not available in push request certificate	Please ensure the private key is available in request
Pivate key In device configured. But key content is available with the certificate from AppViewX.So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Privatekey not exists in device.	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	Ensure the user has permission.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting Paloalto Firewall

This section helps you troubleshoot the common problems that you might encounter while using Paloalto firewall functionalities. This guide will give more troubleshooting processes on Paloalto firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Paloalto firewall.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Invalid parameter for number of bits Csr generation is device failed	Selected EC bit length may not be supported by Paloalto.	Please select valid bit length supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name not given or length less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issues in Backup, Push, Bind and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with the private key to bind with the profile.
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than current time.	Only valid certificates can be pushed.

Troubleshooting Panorama Firewall

This document helps you troubleshoot the common problems that you might encounter when using the Panorama firewall functionalities. This guide will give more troubleshooting processes on Panorama firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Panorama firewall.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Issues in Panorama Firewall Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials

Issues in Panorama Firewall CSR Generation

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid	Provide valid credentials
Unsupported Key type provided	Unsupported key type is selected	Please select RSA or EC
Csr generation is device failed	CSR generation is failed	CSR generation has failed. Please refer to the error message associated with this
1) Invalid parameter for number of bits	Selected EC bit length may not be supported by panorama	Please select valid bit length supported

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
2) Csr generation is device failed		

Issues in Panorama Firewall Backup, Push, Bind, and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with private key to bind with the profile
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than current time.	Currently, valid certificates only can be pushed.

Troubleshooting Check point Firewall

This document helps you troubleshoot the common problems that you might encounter when using the Check point firewall functionalities. This guide will give more troubleshooting processes on Check point firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Check point firewall.

Issues when device goes to unresolved state after on-boarding

The device might have entered an unresolved state due to connectivity issues from the AppViewX installed node or CC node. In such cases, please follow the steps below:

1. Attempt to establish an SSH connection from the AppViewX installed node or CC node to the Check point server.
2. Verify if there is proper connectivity between the nodes and the Check point server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues when device goes to failed state with version failure

When a device enters a failed state with version check failure, it typically indicates that the system is unable to retrieve the version information from the Check point SMS server.

1. Login to the Check point SMS server via CLI using the credentials configured in AppViewX.
2. Attempt to enter expert mode. The user should be able to switch to expert mode.
   • Verify the expert password provided during on-boarding is correct.
   • Confirm expert mode privileges are granted for the user account.
3. Once in expert mode, execute the following command: **`fwm ver`**. This command should confirm the server is indeed a Check point SMS server and display the version details of the server.
   Sample expected output:

```
This is Check Point Security Management Server R81.20 - Build 440
```

Troubleshooting RabbitMQ Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with RabbitMQ server.

Issues in RabbitMQ Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to RabbitMQ Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations:	Problem with port configuration	Check if the configured port in the device addition page is correct.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings		
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMacs configured in the target device and ensure AppViewX SSH-plugin supports the same
Device version fetch has failed.	Config path is incorrect / No RabbitMQ instances running in the target device	Check manually by establishing an SSH session to the target device and check RabbitMQ installations and find a valid configuration path and update the same in the device addition page.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files (/etc/rabbitmq/rabbitmq.config). These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Custom Config Location	For default installation, The config location path is / etc/rabbitmq/rabbitmq. config, if any custom location is provided check the valid rabbitmq config file exists in that location	Login via SSH to the target device and check the “rabbitmq” installations and valid configuration file location path
Permission denied for file/ location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location	1.Check whether someone deleted the file from AppViewX environment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	3.Device communication might not be established when service has started.	2. Verify if read permission is given for the location. 3.Verify the device connection and restart the service.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	Verify the input details and check for device status error messages in the Issues in Communicating to RabbitMQ Server section.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available on device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Rapid SB Server Inventory

This document will help you troubleshoot the issues faced during the use of the functionalities of Rapid SB connectors server inventory. It begins by troubleshooting the common functionalities and then goes on to handle the issues peculiar to various Rapid SB connectors Servers.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location 3.Device communication might not be established when service has started.	1.Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3.Verify the device connection and restart the service.

Issues in Credential List

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Managed Server

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Server

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in an expected format.	Supported file types are CSV/Xls/ xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In the file history of the import page maximum of 5 files can only be maintained.	Delete any of the parsed/completed files to upload a new one.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Export Server

Error Message	Possible Cause	Possible Solution
Exception while exporting	1.General failure - Unable to create file on the local system due to permission issue. 2.Unable to fetch device list from the database.	1. Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.) 2. Make sure the database is running and has correct data.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “**Discover By**” section.	Select at least one device to discover certificates from.

Troubleshooting Rapid SB Linux Server

This section helps you troubleshoot the common problems that you might encounter while using certificate server functionalities for Linux servers. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux servers.

Issues in Linux Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Linux Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can contain only alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name on the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable.	Check manually by establishing a SSH session to the target device with the provided IP/FQDN.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration.	Check if the configured port in the device addition page is correct.
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake.	Request to check the ciphers, key and HMacs configured in the target device and ensure AppViewX SSH-plugin supports the same.

Issues in Accessing the Server

Issues with accessing servers can occur while communicating with servers or discovering or fetching configuration files. These errors can be collected either from logs, API responses or can be seen in the status field for that particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/ location.	1. File might not be present in the avx environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Credential List

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded does not have the correct format.	Provide key file with correct format (.pem or .txt)

Issues in Managed Server

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Unmanaged Server

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) that is in unmanaged state before unmanaging it again.
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) that is in an unmanaged/inprogress state before unmanaging it again.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an inprogress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are csv/xls/xlsx only. Check for the uploaded file extension.
Maximum five files allowed, please delete any completed file.	In file history of import page maximum 5 files can only be maintained.	Delete any of the parsed/completed files to upload a new one.

Issues in Export Server

Error Message	Possible Cause	Possible Solution
Exception while exporting	1. General failure - Unable to create file on the local system due to permission issue. 2. Unable to fetch device list from the database.	1. Provide access to be able to create the file on the local system. (For example, check the directory where it is trying to export and give access to AppViewX for that directory.) 2. Make sure the database is running and has correct data.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due invalid credentials / SSH Port.	Verify the input details and check device status error messages in the Issues in Communicating to Linux Server section.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available in device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Troubleshooting Tomcat Linux

This document helps you troubleshoot the common problems that you might encounter when using Tomcat Linux functionalities. This guide will give more troubleshooting processes on issues related to the Tomcat Linux server. The issues are device addition, communication to the server, CSR generation, access to the server, fetch configuration, discovery along with push and rollback.

Issues in Device Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Device name accepts '-' , '_' , '.' , '*' , '|' , '!' and space only, with min 2 and max 64 characters.	Server name is not valid.	Provide a server name with min 2 and max 64 characters with only the allowed characters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Communicating to the server

Error Message	Possible Cause	Possible Solution
Failed to make the ssh connection with the given IP.	Given IP may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure given IP is connected to the network.
	SFTP port is not open for SSH communication.	Open given port for the SSH communication.
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Device does not belong to Tomcat Server.	Device does not have any running tomcat instances.	Start any tomcat server in the device.
Failed to make ssh connection.	Target device may not be connected to the network.	Validate whether username and password given during device addition are valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Username/Password provided may be incorrect.	Ensure the target device is connected to the network.
	The User may not have permission to execute the command.	Provide permission for the user to execute \"ps -ef\" command.
Linux rest agent communication failed	Rest agent installed in the device might not be running.	Install AppViewX Rest agent in device.
	The Client certificate installed in AppViewX might not be valid.	Install valid client certificate in AppViewX.
	Rest agent port might not be open for communication.	Ensure port is open for communication.
Error while decrypting password.	Password invalid for decryption key.	Check if the password matches with the decryption key.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
CSR Generation Failed.	Given CSR Location is not available in device.	Provide a valid path to store CSR and key.
	User does not have read/write permission for the location.	Ensure the user has read/write permission to the given location.
	“Openssl” package is not installed	Install “Openssl” package in the device
	The User does not have permission to execute “Openssl” commands.	Provide permission for user to execute “Openssl” commands

Issues in Access

Access Issues might occur when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
File Download Failed.	User or User group does not have read/write permission for server.xml in device.	Provide read/write permission for user in device

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
XML Parsing Failure	FileName provided might not be a valid XML file.	Ensure the provided filename is a valid XML file.
File Download Failed.	server.xml is not found in the specified directory.	Ensure server.xml is present in the conf directory.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
File Not Found	server.xml is not present in the specified directory.	Ensure server.xml is present in the conf directory.
	SSL certificate or key file parsed from configuration file is not present in the specified directory.	Ensure parsed certificate or key file is present in the directory specified in server.xml
JKS Parsing Failure	Password for Keystore file may not be present in server.xml	Password given in server.xml might be incorrect.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Push failed.	Creating local certificate files failed while Backup.	Provide required access to AppViewX to create local files

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate Push Failure	Invalid certificate, key, or trust location is given.	Provide the valid certificate, key, or trust location while adding an application connector.
Bind Failed as the SSL is disabled for the port	SSL is disabled for the given port on the server.	Kindly enable SSL for the port on the server.
KeyStore creation failed	Unable to create the Keystore locally.	Provide required access to AppViewX to create local files

Troubleshooting Weblogic Linux

This section helps you troubleshoot the common problems that you might encounter when using Weblogic Linux functionalities. This guide will give more troubleshooting processes on issues related to Weblogic Linux server. The issues are device addition, communication to the server, CSR generation, fetch configuration, discovery along with push and rollback.

Issues in Device Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Weblogic Linux

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for device cannot be empty.	Access list provided is empty	Provide a valid access list to communicate with the device.
Username cannot be null or empty.	Username is null or empty.	Provide a valid username to communicate with the device.
Password cannot be null or empty.	Password is null or empty.	Provide a valid password to communicate with the device.
Key cannot be null or empty.	Key is null or empty.	Provide a valid key to communicate with the device.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches with the key.
Failed to connect to the server.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
No weblogic process is running	Weblogic processes running on the destination machine might be down.	Kindly check the status of the Weblogic process running in the destination machine.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Domain-registry.xml is not accessible in the given path.	Given path may be invalid or AppViewX does not have	Please enter a valid path or Check permissions to access the file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	permission to access the file in the path.	
Config file parsing failed.	1. Configuration file might be corrupted/ empty. 2. AppViewX is not able to read/ parse the Config files from the server.	1. Verify if the configuration file is correct. 2. Check if the server has proper config files related to the Weblogic server and AppViewX has proper read permissions.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not entered or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception while fetching key and location details from request.	Certificate location details provided during the server addition might be wrong.	Check and provide the valid certificate location during server addition.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Provide valid credentials to communicate with the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Error occurred while creating conf file to create csr.	AppViewX is not able to create a conf file in the export directory.	Check if AppViewX export directory has write permissions.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Provide valid credentials to communicate with the device.
Unable to parse configuration to fetch currently associated data.	AppViewX may not be able to fetch and parse the content of the certificate which is already associated.	Check if AppViewX has permissions for fetching the existing certificate content.
No server certificate is found	AppViewX may not be able to fetch and parse the content of the certificate which is already associated.	Check if AppViewX has permissions for fetching the existing certificate content.
Exception while downloading trust store / Exception while parsing certificate	AppViewX is not able to download the trust store from the server.	Check if AppViewX has permission to download the trust store from the device.
Certificate and/or key missing	Certificate provided in the push request might be invalid.	Check if the certificate that is being pushed is valid.
Unsupported Key Algorithm	Key algorithm of the certificate is not supported by the server.	Provide a valid key algorithm that is

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		supported by Weblogic servers.
Push cannot be performed automatically for the Keystore type 'DemoIdentityAndDemoTrust'. Kindly customize the keystore locations in the connector.	Customize push location not provided during push operation.	Provide a location to push the certificate inside the server.
Parsing a certificate is failed	Certificate content might be invalid.	Check the certificate content.
Exception while writing file to avx local.	AppViewX may not have access to the local/export directory.	Check if AppViewX has permission for the local/export directory.
Certificate push is failed.	Invalid location provided. User is not having permission to push file to the location.	Check the location provided is valid. Check if the user has permission to access the location.
Unable to perform Bind for the server.	Server may not be running in the given address and port.	Check if the server is running in the given port and listen address
Unable to open edit session for the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to perform edit for the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the server credentials are valid.
Unable to save the current changes made to the server.	AppViewX is not able to communicate with the server.	Check if the server is up and running and the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
		server credentials are valid.
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state. Previous work order is in progress and not completed. AppConnector might not be in sync.	Push to device after certificate has been retrieved from CA. Initiate push after previous work order is finished. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/ rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Websphere Linux

This section helps you troubleshoot the common problems that you might encounter when using Websphere Linux functionalities. This guide will give more troubleshooting processes on issues related to Websphere Linux server. The issues are device addition, communication to the server, CSR generation, fetch configuration, discovery along with push and rollback.

Issues in Device Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might either be missing or might be invalid.	Add all the valid information in the mandatory section.
WSadmin User name and WSadmin Password should not be empty	WSadmin username or password might be empty.	Add the valid WSadmin username and password.
Kindly add at least one WSadmin detail before saving.	WSadmin details are not added.	Add at least a single WS admin details.

Issues in Communicating to Apache Linux

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for device cannot be empty.	Access list provided is empty	Provide a valid access list to communicate with the device.
Username cannot be null or empty.	Username is null or empty.	Provide a valid username to communicate with the device.
Password cannot be null or empty.	Password is null or empty.	Provide a valid password to communicate with the device.
Key cannot be null or empty.	Key is null or empty.	Provide a valid key to communicate with the device.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches with the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Ip does not belongs to Websphere	Destination machine might not have the required configuration for a Websphere application server.	Please check if the machine has Websphere configurations available in the destination machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide proper credentials to communicate with the device.
Permission denied to installation path.	AppViewX may not have the permission for the installation path.	Check if AppViewX has permission to access the installation path.
Invalid Credentials.	Invalid Credentials given for installation path.	Check if credentials have access to the installation path.
Permission denied	User does not have provision to access the installation path.	Check if AppViewX has permission to access the installation path.
Invalid installation path	Installation path does not exist.	Check if the installation path provided is a valid one.
Wsadmin objects unavailable	Wsadmin objects are unavailable	Check if the configurations related to WS are available in the destination machine.
security.xml file read operation failed	security.xml is not accessible in the given path.	Check if there is permission to access the file.
Config file parsing failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or its length is less than 2 characters.	Enter a valid name with a minimum of 2 characters. Provide a time interval between batches in minutes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Interval between batches info. is missing when execution type is sequential.	
Please select a device	No device is selected in the “Discover By “section.	Select at least one device to discover certificates from.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Service account user not found.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Authentication failure using Service account.	Credentials to communicate with the device may be invalid.	Check and provide the proper credentials to communicate with the device.
Permission denied to installation path.	AppViewX may not have the necessary permission for the installation path.	Check if AppViewX has permission to access the installation path.
Invalid Credentials.	Invalid Credentials are given to installation path.	Check if credentials have access to the installation path.
Permission denied	User does not have provision to access the installation path.	Check if AppViewX has permission to access the installation path.
Invalid installation path	Installation path does not exist.	Check the installation path provided is a valid one.
Wsadmin objects unavailable	Wsadmin objects unavailable	Check if the configurations related to WS are available in the destination machine.
security.xml file read operation failed	security.xml is not accessible in the given path.	Check for valid permission to access the file.
Config file parsing failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Error while establishing SSH connection.	AppViewX is not able to establish a SSH connection using the given credentials.	Check and provide valid credentials to communicate with the device.
Error occurred while creating conf file to create csr.	AppViewX is not able to create a conf file in the export directory.	Check if AppViewX export directory has write permissions.
Invalid key type specified in the request	Given key type might not be supported in the target machine.	Provide valid key type.
CSR and Private key has been failed.	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
security.xml file read operation failed	AppViewX may not be able to read security.xml of the profile.	Check if AppViewX has permissions to read security.xml of the profile.
Config file parsing failed	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
Insufficient information to fetch backup data available in the server.	Configuration files fetched from the server may not have sufficient information.	Check if the config file has all the information related to server configuration.
Unsupported bit length	Bit length is not supported by the server.	Provide a valid bit length that is supported by Websphere server.
Unsupported Key Algorithm	Key algorithm of the certificate is not supported by the server.	Provide a valid key algorithm that is supported by Websphere servers.
Creating local certificate file failed - <Detailed Message>	AppViewX is not able to create file in a temporary folder.	Check the detailed message to determine the remedy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Server certificate is not available to push.	Server certificate location may be invalid.	Check if the trust store location is available.
Private Key doesnot exists for certificate	Private key may not be available for the certificate.	Check if the private key for the certificate is available.
Private key parsing failed for the certificate.	Private key may be a invalid one.	Check if the private key is valid.
Writing of converted certificate related files into file in AppViewX local directory is failed.	AppViewX may not have permission to write a file in the export directory.	Check if AppViewX has proper permissions for the export directory.
Certificate created date is earlier than server present time	The starting of certificate validity period is earlier than the servers present time.	The starting of certificate validity period should match with the server's time. It should be greater than the server's present time.
Unsupported Type	Certificate format is not supported by the server.	Check for the supported certificate formats.
Error found in wsadmin response	The WSadmin console may not be working on the server.	Kindly check WSadmin console is properly working or not
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Troubleshooting Websphere Windows

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Websphere Windows.

Issues in Server Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Connecting to remote server ptpld123 failed with the following error message : The user name or password is incorrect. For more information, see the about_Remote_Troubleshooting Help topic.	Invalid hostname/ Invalid credential	Kindly check if the given host is reachable. Kindly provide valid credentials and update the device details.
Communication to <host> failed.	Windows Agent is not reachable or down	Kindly check if windows agent configured and in running state.
Websphere version fetch has failed	Websphere setup is not available/not configured in given device	Kindly validate is Websphere configured properly

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch.	1. No valid keystore files available in the given path. 2. Users don't have access for the configured location/file. 3. Web Server or WAS console is not active.	1. Kindly Ensure the given certificate location has a valid cert. 2. Kindly ensure users have proper access privilege to read certs. 3. Kindly ensure WebServer is in up and running state .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Error while pushing certificate into device.	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
Error while pushing certificate into device : Websphere due to Unsupported bit length:4096.	Websphere will support bitlength up to 2048.	Kindly ensure the certificate issued is compatible with the Websphere.
Error while pushing certificate into device : Websphere due to Unsupported Key Algorithm:DSA	Unsupported key Algorithm.	Kindly ensure the certificate issued is compatible with the Websphere.
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key. If privatekey is available in the device please select privateKeyInDevice option.

Troubleshooting Windows Apache Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Apache server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Device communication failed	1. Given credential is incorrect. 2. Windows agent may not be working. 3. Device not reachable 4.Hostname value is in-correct	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable 4. Ensure windows agent is working for communication mode gateway 5. When the communication mode selected is SSM, Ensure SSM details given are correct

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Push failed due to Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request
Push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Push failed due to Private key is not available in device. Failing the push	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have the permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Troubleshooting Windows JBoss Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows JBoss server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Windows JBoss Server Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Windows JBoss Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct details and click Save.
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Error on fetching JBoss instance, config fetch process failed due to No configuration file found. Check installation directory path.	Provided installation directory path does not have JBoss configuration files like server.xml / standalone.xml	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Error on fetching JBoss instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid installation directory path	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.

JBoss version fetch is failed	No JBoss server running in the target device / something wrong in the JBoss installation	Login manually into the windows server and find the
		JBoss server bin directory and run the below command to validate the JBoss version
		For JBoss 4.0.5
		`<JBoss_server_Directory>/bin/run.bat -V`
		For JBoss 6.4 and 7.0
		`<JBoss_server_Directory>/bin/standalone.bat -V`
		Currently only JBoss 4.0.5, 6.4 and 7.0 versions are supported in AppViewX.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from the environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Verify the input details and check for device status error messages in the Issues in Communicating to Windows JBoss Server section.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/ write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	"Private key in Device" is enabled in application connector and also private key is available in the certificate	Ensure to uncheck "Private key in Device" attribute in application connector
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector,	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	but key is not available in device.	certificate is generated using CSR gen option from Device.

Troubleshooting Windows Weblogic Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Weblogic server.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Device communication failed	1. The given credential is incorrect. 2. Device not reachable 3.Hostname value is incorrect	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable
Error while communicating via windows agent service	Windows agent not reachable	Ensure windows agent is running and it's accessible
Version fetch failed and Fetch weblogic instance failed	Given “Weblogic Installation directory” is in-correct	Check and ensure the given installation path is correct

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	1.Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request
Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Private key is not available in device. Failing the push	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 6: Key Use Cases

- Automating CLM for Akamai CPS
- Automating CLM for Apache (Linux)
- Automating CLM for Apache (Windows)
- Automating CLM for Tomcat (Linux)
- Automating CLM for Tomcat (Windows)
- Automating CLM for JBoss
- Automating CLM for Linux
- Automating CLM for Windows Environment
- Automating CLM for Microsoft IIS
- Automating CLM for Firewall
- Automating CLM for Palo Alto
- Automating CLM for CheckPoint
- Automating CLM for F5 Devices
- Automating CLM for Citrix Devices
- Automating CLM for AWS Resources
- Automating CLM for Microsoft Azure Resources
- Automating CLM for Microsoft SQL
- AppViewX Integration with MDM devices

Automating CLM for Akamai CPS

The Akamai CPS (Certificate Provisioning System) provides the full lifecycle management of SSL/TLS certificates for Akamai Secure Delivery Network applications.

Prerequisites

- Follow Create authentication credentials to generate client token, client secret, and access token required to authenticate to Akamai CPS.
- To enable this API, choose the **Certificate Provisioning System** API service, and set the access level to **READ-WRITE**.
- Ensure your API credentials have the following grants: **CPS** and **Contracts-API_Contracts**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The user must have **Access to the Property Manager API (PAPI)**.
- Ensure the user's **PAPI access level** is set to **READ** to allow read operations through the API.

Onboarding Akamai CPS Device

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **+ (Add)** icon.
4. Select **Akamai** from the Vendors list.
   The **Akamai** server configuration screen is displayed.
5. In the **Server Details** section, enter details as mentioned:

Server Details - Field Description Table

Field	Description
***Server name**	Enter a unique name for server.
***IP address/ FQDN**	Enter a valid IP address or FQDN for device communication and integration with the Akamai CPS.
Data center	Choose the desired data center.
Proxy required	Select the checkbox to enable the secure proxy service.
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter details as mentioned below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Field	Description
***Client token**	Enter the client token as provided by the vendor.
***Client secret**	Enter the client secret as provided by the vendor.
***Access token**	Enter the access token as provided by the vendor.
***API Version**	Enter the value, example cps/v2. (The same value is provided as the placeholder.)
**: Mandatory fields*	

7. Click **Save**.
   The Akamai CPS device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to (**Menu**) > **CERT+** >**ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Configuring Device Settings

During enrollment using server device as endpoint, Akamai has a long list of details that are mandatorily required for the enrollment request. Adding these fields along with the CSR parameters will make the enrollment form too big with many details to be filled out. As these are fixed values and only have to be filled once, the other mandatory fields are made available in the global device settings page. The details

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

saved on the global setting page are based on the combination of the fields **Validation Type**, **Secure Network**, and **Vendor Certificate Type** that are available on the enrollment page.

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the (**Device Settings**) icon.
4. Select **Akamai** from the Vendors list.
   The Akamai Vendor Specific Details configuration screen is displayed.
5. Enter the fields in the respective sections as described:

Filed descriptions for the Vendor Specific Details page

Field	Description
General Information	
***Validation Type**	Select a validation type from the dropdown list for the endpoint. The default value is **Third-party**.
***Secure Network**	This filed helps identify the type of deployment network. Select the secure network from the dropdown list for the endpoint. The default value is **Standard TLS**.
***Vendor Certificate Type**	Denotes the domain and organization validation type. Select a vendor certificate type from the dropdown list for the endpoint. The default value is **Third-party**.
Organization Information	
***Name**	Enter the organization's name.
***Address**	Enter the organization's address.
***Country**	Enter the organization's country code.
***City/Municipality**	Enter the organization's city or municipality.
***State/Province**	Enter the organization's state or province.
***Zip/Postal Code**	Enter the organization's zip or postal code.
***Phone Number**	Enter the organization's phone number.
Admin Contact Information	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	Enter the administrator's first name
***Last Name**	Enter the administrator's last name
***Phone Number**	Enter the administrator's phone number
***Email**	Enter the administrator's email
Tech Contact Information	
***First Name**	Enter the technical contact's first name
***Last Name**	Enter the technical contact's last name
***Phone Number**	Enter the technical contact's phone number
***Email**	Enter the technical contact's email
*: *Mandatory fields*	

6. Click **Update**.
   The vendor details are saved successfully.

Enrolling Server Certificates

Prerequisite

- Before proceeding with the endpoint enrollment for Akamai CPS, the **Device Settings** configuration is a must.

Note:

- The product supports the enrollment and deployment of certificates for a **single stack**. The **CSR content** is generated based on the key type selected on the enrollment page.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. Specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. Specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** • This value can exceed the certificate's validity in case of short-lived certificates. • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
***Certificate Type**	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for DigiCert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a CA+RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Select **Browse** and navigate to the location of your CSR file, and click **Open**.. b. Click **Upload**. • **HSM**: **Note:** This option is not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given, in an HSM device: a. Under **CSR Generation**, select **HSM**. b. Fields for gathering your HSM-related inputs are displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
To generate the private key and the CSR, enter the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated:
• HSM Devices
• ADC Devices</td></tr>
<tr><td>*Vendors</td><td> Note: This field is applicable only when Device Type = ADC Devices.</td></tr>
<tr><td>*Devices</td><td>From the dropdown list, select the required HSM/ ADC device.
 Note: This field is populated based on the Device Type and Vendors selected.</td></tr>
<tr><td>*Key Handler Name</td><td> Note: This field is applicable only when Device Type = HSM Devices.
Enter the key handler name.</td></tr>
<tr><td>*Key Reference Name</td><td> Note: This field is applicable only when Device Type = ADC Devices.
Enter the key reference name.</td></tr>
</table>
• End Point:
Note: This option is disabled when Certificate Authority = Google and CSC Global.
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To generate the private key and the CSR in the selected end point device, enter the following inputs:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Category</td><td>Select Server from the dropdown list.</td></tr>
<tr><td>Vendor</td><td>Select AkamaiCPS from the dropdown list.</td></tr>
<tr><td>*Devices</td><td>This field is auto-populated.</td></tr>
<tr><td>*Contract ID</td><td>This field is auto-populated if you have configured device settings.</td></tr>
<tr><td>*Validation Type</td><td>This field is auto-populated if you have configured device settings.</td></tr>
<tr><td>*Secure Network</td><td>This field is auto-populated if you have configured device settings.</td></tr>
<tr><td>*Vendor Certificate Type</td><td>This field is auto-populated if you have configured device settings.</td></tr>
</table></td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
*: Mandatory fields	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. For the certificate being enrolled, enter the **CSR Parameters**.

> **Note:** For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except underscore (_) and hyphen (-).
Subject Alternative Name	From the dropdown list, select the Subject Alternative Name category for the certificate being enrolled. In the corresponding field(s) displayed for the selection made, enter the required values. **Note:** • Multiple values must be separated by a comma. • After enrollment, the cumulative count of SANs is displayed in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** For renewal of the certificate being enrolled, country name is required.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you've uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, provide the organization-specific values for both the certificate attributes and the custom attributes required by the issuing CA to be included with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

   Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

    Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding Application Connector

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.
***Vendor**	From the dropdown list, select **Akamai CPS**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Akamai CPS server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Type	From the dropdown list, select the file type of the certificate to be pushed. For Akamai CPS, by default, the **PEM (*.pem)** certificate is selected and the dropdown list is non-editable.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on the end device, select this checkbox. For Akamai CPS, this feature is enabled by default and the field is non-editable.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For Akamai CPS, this feature is enabled by default and the field is non-editable.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing Server Certificates to Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:**
> - The **Push to Device** option is displayed only after an application connector is added to certificate.
> - Certificate deployment to the staging environment is only currently supported.
> - **Renewal of existing enrollments** with updated certificates is also **not supported** at this time.

The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- If you want to discover certificates from the onboarded device, see Managed Devices Scan.

Automating CLM for Apache (Linux)

Apache on Linux Servers is a widely used configuration for hosting websites and applications due to its open-source nature and strong performance. Linux offers a stable and secure environment, allowing

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Apache to run efficiently and be customized to meet specific needs. The combination benefits from extensive community support, regular updates, and a wide range of available modules. Linux's command-line interface facilitates powerful management and automation of Apache. This setup is often used in LAMP stacks, making it a popular choice for dynamic web hosting.

Prerequisites

1. Ensure that application/service users have the appropriate read/write permission to perform the CLM actions on the server device, if the access elevation is selected as **None**.
   When the access elevation is **sudo** or **dzdo**, all the commands used to perform the CLM operations will be executed with sudo or dzdo.
2. Verify that the commands needing sudo or dzdo access have been enabled on the server.
3. Ensure that the following packages are installed to facilitate device addition:
   • sudo/dzdo (optional, as per the access elevation selected)
   • timeout
   • base64
4. Ensure that the target IP address is accessible from the cloud connector and the port is open.
5. Make sure that the language setting for the Apache Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
6. Only certifiticates in .pem, .crt, and .cer formats and key files are discovered.
7. SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
8. Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.
9. Verify the existence of **httpd.conf** file in the system by scanning from root directory. Use the command: find / -name “httpd.conf”.
10. Check for the ServerRoot location in the **httpd** file. Make sure it holds forward slashes(/) as path separator as in other Linux-based file locations. (This might lead to failure in managing Apache server installed on the Windows machines).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Apache Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Linux** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Apache** radio button.
***Server name**	Enter the name of the designated Linux server.
***IP address/ FQDN**	Enter the IP address of the Apache Server or its fully qualified domain name (FQDN) that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the Apache server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.

   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - AppViewX* • *SSH* **Note:** • If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. (The field label changes to ***Account Name** if **SSM** is the communication mode)
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Access Elevation**	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/ dzdo.
File Upload Temp Path	This field is displayed when the *Access Elevation* = *sudo or dzdo*. Enter the temporary directory/path where certificates or keys are stored during certificate push actions. *Example*: /tmp/files **Note:** It is used as an intermediate location to store the actual keystore and then perform actions on the certificates in the keystore. The keystore is then moved back to the original location after performing the actions.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
Account number	Enter the 12-digit AWS account number. *Example*: 012345678901

8. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Certificate location	Enter the actual directory/path where certificates are stored in the Apache server. *Example*: /cert/files
Key location	Enter the actual directory/path where keys are stored in the Apache server. *Example*: /key/files
Intermediate location	Enter the temporary or intermediate directory/path where certificates and keys are stored in the Apache server. *Example*: /inter/files

9. Click **Add**.
   Once the server is added successfully, the certificate location will be listed in the table.
10. *(optional step)* Click the (Delete) icon, if you want to delete the certificate details from the list.
11. Click **Save**.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Certificates for Apache Linux Server

Discovering Certificates for Apache

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

   Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

   Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to the Apache Linux Server

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for a Apache Linux Server

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Apache**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Apache (Linux) server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Service Restart	To restart the Apache service immediately after the certificate is pushed, enable this checkbox.
Suppress Heartbeat Alerts During Service Restart	Enabling this option to disable or prevent false alert triggered during Apache service. **Note:** • This field is disabled when Service Restart selected. • To view or update default setting, go to: **Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings**.
Heartbeat File Path	Specify the hearbeat file path. **Note:** This field is enabled when Suppress Heartbeat Alerts During Service Restart is checked.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
Intermediate Location	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the path to the location on your local system where the intermediate certificate file is stored.
Root Location	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the path to the location on your local system where the root certificate file is stored.

5. Enter the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Apache Linux Server

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

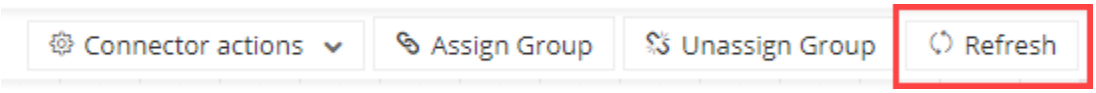
- The approval process is triggered. The current flow is based on the default policy of two-level approvals.
- A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

d. Click **Update**.

2. To enable auto renewal for the certificate connector:

a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
The **Server Certificate** inventory is displayed.

b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
The holistic view of the selected certificate is displayed.

c. For an existing CA connector for the certificate, hover over .

d. From the menu displayed, click **Edit**.
The certificate details are displayed.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Apache Linux

This document helps you troubleshoot the common problems that you might encounter when using Apache Linux functionalities. This guide will give more troubleshooting processes on issues related to Apache Linux server. The issues are device addition, communication to the server, CSR generation, access to server, fetch configuration, discovery along with push and rollback.

Issues in Device Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating with the Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device ip/fqdn as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Ip is not reachable/invalid.	Invalid credentials	Kindly check the credentials provided.
	IP is not reachable	Kindly check if IP is pingable or not and make it up and running.
	IP is blocked by the firewall	Kindly check firewall settings.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Communication Failed	Username or password may be invalid	Check and provide the correct username and password.
java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods.	Authentication Failure	Provide correct credentials for authentication. Make sure SSH is enabled on the given server.
Linux rest agent communication failed.	Rest agent running on the destination machine might be down.	Please check the status of the rest agent in the destination machine.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.

Issues in Access

Access Issues occur while communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/location.	File might not be present in the avx environment.	Check whether someone deleted the file from AppViewX environment.
	user might not have permission to read in the given source location.	Verify if read permission is given for the location.
	Device communication might not be established when service has started.	Verify the device connection and restart the service.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Parsing apache configuration failed.	Configuration file might be corrupted/ empty.	Verify if the configuration file is correct.
	AppViewX is not able to read/ parse the Config files from the server.	Check if the server has proper config files related to Apache Server and AppViewX has proper read permissions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not entered or the length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Automating CLM for Apache (Windows)

Apache on Microsoft Windows Servers is ideal for organizations using a Windows-based infrastructure, offering robust web server capabilities with seamless integration into the Microsoft ecosystem. It works well with Windows-specific services like Active Directory and SQL Server, providing a consistent platform for enterprises. Although Apache was originally designed for Unix-like systems, it is fully compatible with Windows and runs efficiently in this environment. Windows provides a user-friendly interface for managing Apache, making it accessible to administrators familiar with Microsoft tools. This setup is commonly used for hosting websites and applications that require integration with other Windows services.

Prerequisites

1. Ensure that application/service users have the appropriate read/write permission to perform the CLM actions on the server device, if the access elevation is selected as **None**.
   When the access elevation is **sudo** or **dzdo**, all the commands used to perform the CLM operations will be executed with sudo or dzdo.
2. Verify that the commands needing sudo or dzdo access have been enabled on the server.
3. Ensure that the following packages are installed to facilitate device addition:
   - sudo/dzdo (optional, as per the access elevation selected)
   - timeout
   - base64
4. Ensure that the target IP address is accessible from the cloud connector and the port is open.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Make sure that the language setting for the Apache Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
6. Only certifiticates in .pem, .crt, and .cer formats and key files are discovered.
7. SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
8. Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.
9. Verify the existence of **httpd.conf** file in the system by scanning from root directory. Use the command: find / -name “httpd.conf”.
10. Check for the ServerRoot location in the **httpd** file. Make sure it holds forward slashes(/) as path separator as in other Linux-based file locations. (This might lead to failure in managing Apache server installed on the Windows machines).

Onboarding Apache Windows

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Microsoft** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Apache** radio button.
***Server name**	Enter the name of the designated Apache server.
***Hostname**	Enter the hostname of the Apache Server that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Apache server. Gateway is the preferred communication mode.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - AppViewX **Note:** If **Credential list - AppViewX** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

   If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\Apache-Tomcat-8.5.35
***Region**	Enter the geographic region of the AWS instance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

8. Enter the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations). Prerequisites for using the Integrated Windows Gateway mode **Note:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Gateway location**	From the following options, select the gateway location: • **Remote** **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. From the following options, select the gateway: • New • Existing
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

9. Click **Save**.
   The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Onboarding Certificates for Apache Linux Server

Discovering Certificates for Apache

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Apache Windows Server Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Apache Windows

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows Apache**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Windows Apache devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Enter the path to the location on your local system where the certificate file to be pushed is stored.
***Key Location**	The private key associated with a certificate is stored in a key file. In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
Intermediate Location	Enter the path to the location on your local system where the intermediate certificate file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Root Location	Enter the path to the location on your local system where the root certificate file is stored.
Service Restart	To restart the Apache service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

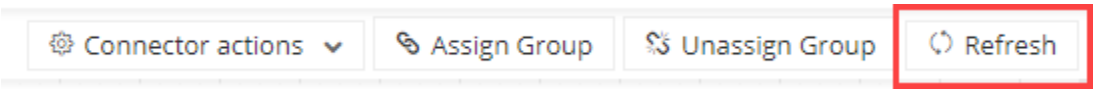
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
The **Server Certificate** inventory is displayed.

b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
The holistic view of the selected certificate is displayed.

c. For an existing CA connector for the certificate, hover over .

d. From the menu displayed, click **Edit**.
The certificate details are displayed.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Troubleshooting Windows Apache Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows Apache server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Device communication

Error Message	Possible Cause	Possible Solution
Device communication failed	1. Given credential is incorrect. 2. Windows agent may not be working. 3. Device not reachable 4.Hostname value is in-correct	1. Check and input the correct credential. 2. Check and input the correct hostname value 3. Ensure the device is reachable 4. Ensure windows agent is working for communication mode gateway 5. When the communication mode selected is SSM, Ensure SSM details given are correct

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	1. Device not running or not accessible 2. No valid certificates available	1. Ensure target device is up and running 2. Check the device has valid certificate files

Issues in CSR generation at Endpoint

Error Message	Possible Cause	Possible Solution
CSR generation got failed/User has no permission for the given location to perform the operation.	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Push

Error Message	Possible Cause	Possible Solution
Push failed due to Private key is not available. Failing the push	Private key not available in push request certificate	Please ensure the private key is available in request
Push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	Trying to push a certificate with key when the “Private key in device” enabled	Ensure the push certificate has no key when “Private key in device” is enabled.
Push failed due to Private key is not available in device. Failing the push	Private key file not available in the given key location when “Private key in device” is enabled	Ensure the target device has key file in the given location
Push failed since cannot write-into/create location(s)	User does not have the permission to perform the operation	1.Ensure the user has permission. 2.For sudo user, please check the access elevation value given in device addition
Device is not in managed state	Device is not available in managed	Please check the device status in device inventory

Automating CLM for Tomcat (Linux)

Tomcat on Linux Servers is a popular configuration for running Java-based applications, known for its open-source flexibility and robust performance. Linux provides a secure and stable environment, enabling Tomcat to operate efficiently and be tailored to specific requirements. This combination benefits from strong community support, regular security updates, and a variety of configuration options. Linux’s command-line interface simplifies the management and automation of Tomcat services. Frequently used in conjunction with other components like databases and web servers, this setup is a preferred choice for deploying dynamic enterprise applications.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

- **General Prerequisites**
  - Ensure that the following packages are installed to facilitate device addition:
    - sudo/dzdo (optional, as per the access elevation selected)
    - timeout
    - base64
  - Ensure that the target IP address is accessible from the cloud connector and the port is open.
  - Make sure that the language setting for the Tomcat (Linux) Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
  - Only certificate and key files in PEM, CRT, CER, and JKS formats are detected.
  - SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
  - Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible
- **Prerequisites for Service Account Preparedness**
  - Ensure that access elevation is enabled for the service account.

    When using a service account, all command executions related to the specified use cases occur within the context of the service account. The selected access elevation is relevant only when switching to the service account using a command like:

    ```
    sudo su - serviceAccountUserName
    ```

    When configuring the service account username with access elevation, an option becomes available to enable access elevation for the service account. Enabling accesselevation allows commands to be executed with the selected elevation level.

    If disabled, commands run without access elevation. If enabled, commands are executed with the chosen access elevation and may require a password, depending on the `sudo/dzdo` settings.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If a password is required, ensure that the service account password is entered in the interface when prompted.

Note: If an SFTP connection is set up for the current user, they may not have the requisite access to the service account's directory. It is recommended to configure a dirctory path in the **File Upload Temp Path** in the UI where both the current user and the service account user have read and write access.

Onboarding Tomcat (Linux) Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Linux** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server Type**	Select the **Tomcat** radio button.
***Server name**	Enter the name of the designated Apache Tomcat server.
***IP address/ FQDN**	Enter the IP address of the server or its fully qualified domain name (FQDN) that is to be onboarded.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the server.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Cert Sync	Choose from any of the following: • **Managed** - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • **Monitored** - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • **Ignored** - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *SSH* **Note:** • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - cloudAccount* **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Service account credentials** section, enter the **Username** and **Password** for logging into the service account.
   A service account is a dedicated Linux user account created to run and manage the Tomcat application securely, with controlled access and credential management.
8. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Access Elevation**	Select from the following:. • *sudo* - to execute with root privileges using sudo access • *dzdo* - to execute with root privileges using dzdo access **Note:** SSH key-based authentication doesn't support password enabled sudo/ dzdo.
File Upload Temp Path	This field is displayed when *Access Elevation* = *sudo or dzdo*. Enter the temporary directory/path where certificates or keys are stored during certificate push actions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: /tmp/files
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
Region	Enter the geographic region of the AWS instance. *Example*: us-east-2
Instance id	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
SSM document name	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
SSM document version	Specify the version of the SSM document to be executed. *Example*: 1
S3 bucket name	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

9. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Fields	Description
Server path	Enter the directory/path where the application is installed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: /opt/tomcat/apache-tomcat-9.0.52

10. Click **Add**.
    Once the server is added successfully, the certificate location will be listed in the table.
11. *(optional step)* Click the (Delete) icon, if you want to delete the location details from the list.
12. Click **Save**.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the Status column.
   The status will be set to **Managed/Ignored** if the connection is successful or to **Failed/Unresolved** in case of failure.
4. From the **Status** column, click the **Managed/Ignored/Failed/Unresolved** status value.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Parsing Download Communication File**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Onboarding Certificates for Tomcat Linux Server

Discovering Certificates for Tomcat

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling Server Certificates

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to the Tomcat Linux Server

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for a Tomcat Linux Server

Prerequisites

- **SFTP** is used for the push operations. Ensure that the SFTP port is open to upload or push the certificate to the target machine.

Adding an Application Connector for Tomcat (Linux)

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Tomcat**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Tomcat devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing **server.xml** file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
***Certificate Type**	This field is displayed when **Use Existing Configuration** is not selected. From the dropdown list, select the file type of the certificate to be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Location**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **PEM (*.crt)/PEM (*.cer)/PEM (*.pem)**. This field is displayed when the **Use Existing Configuration** is disabled.
***Key Location**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **PEM (*.crt)/PEM (*.cer)/PEM (*.pem)**. The private key associated with a certificate is stored in a key file. In this field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***KeyStore Location**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **JKS (*.jks)/Default JKS (*.jks)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **JKS (*.jks)/Default JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	This field is displayed when **Use Existing Configuration** is not selected and when **Certificate Type** = **JKS (*.jks)/Default JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Service Restart	To restart the Tomcat service immediately after the certificate is pushed, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	This field is displayed when **Use Existing Configuration** is not selected. To push the root and intermediate certificates, along with the end certificate, select this checkbox.
***Root Location**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **Pem (*.crt)/Pem (*.cer)/Pem (*.pem)**. Enter the path to the location on your local system where the root certificate file is stored.
***Intermediate Location**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **Pem (*.crt)/Pem (*.cer)/Pem (*.pem)**. Enter the path to the location on your local system where the intermediate certificate file is stored.
***Truststore Location**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **JKS (*jks)**. For JKS certificates, the root and intermediate certificates are stored in a truststore file. In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **JKS (*jks)**. Enter the password required to access the truststore file for the JKS certificate to be pushed.
***Truststore File Name**	This field is displayed when **Use Existing Configuration** is not selected, when **Push Root and Intermediate Certificates** is enabled, and when **Certificate Type** = **Default JKS (*jks)**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the name of the truststore file for the JKS certificate to be pushed.

5. Enter/select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

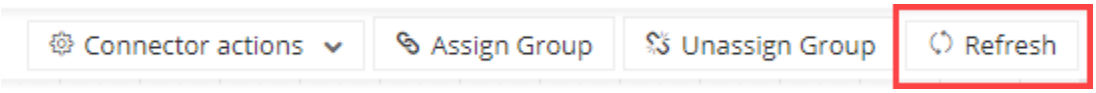
- The approval process is triggered. The current flow is based on the default policy of two-level approvals.
- A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

d. Click **Update**.

2. To enable auto renewal for the certificate connector:

a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
The **Server Certificate** inventory is displayed.

b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
The holistic view of the selected certificate is displayed.

c. For an existing CA connector for the certificate, hover over .

d. From the menu displayed, click **Edit**.
The certificate details are displayed.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Tomcat Linux

This document helps you troubleshoot the common problems that you might encounter when using Tomcat Linux functionalities. This guide will give more troubleshooting processes on issues related to the Tomcat Linux server. The issues are device addition, communication to the server, CSR generation, access to the server, fetch configuration, discovery along with push and rollback.

Issues in Device Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Device name accepts '-' , '_' , '.' , '*' , '|' , '!' and space only, with min 2 and max 64 characters.	Server name is not valid.	Provide a server name with min 2 and max 64 characters with only the allowed characters.

Issues in Communicating to the server

Error Message	Possible Cause	Possible Solution
Failed to make the ssh connection with the given IP.	Given IP may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure given IP is connected to the network.
	SFTP port is not open for SSH communication.	Open given port for the SSH communication.
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Access list for the device cannot be empty.	Credentials not provided for SSH communication.	Provide valid credentials for SSH communication.
Username cannot be null or empty.	Username is not provided or is empty.	Provide a valid username.
The Password cannot be null or empty.	Password is not provided or is empty.	Provide a valid password.
Key cannot be null or empty.	Key is not provided or is empty.	Provide a valid SSH key.
Password / key Mismatch or incorrect.	Unable to decrypt the password with the given key.	Provide a valid password that matches the key.
Device does not belong to Tomcat Server.	Device does not have any running tomcat instances.	Start any tomcat server in the device.
Failed to make ssh connection.	Target device may not be connected to the network.	Validate whether username and password given during device addition are valid.
	Username/Password provided may be incorrect.	Ensure the target device is connected to the network.
	The User may not have permission to execute the command.	Provide permission for the user to execute \"ps -ef\" command.
Linux rest agent communication failed	Rest agent installed in the device might not be running.	Install AppViewX Rest agent in device.
	The Client certificate installed in AppViewX might not be valid.	Install valid client certificate in AppViewX.
	Rest agent port might not be open for communication.	Ensure port is open for communication.
Error while decrypting password.	Password invalid for decryption key.	Check if the password matches with the decryption key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
CSR Generation Failed.	Given CSR Location is not available in device.	Provide a valid path to store CSR and key.
	User does not have read/write permission for the location.	Ensure the user has read/write permission to the given location.
	“Openssl” package is not installed	Install “Openssl” package in the device
	The User does not have permission to execute “Openssl” commands.	Provide permission for user to execute “Openssl” commands

Issues in Access

Access Issues might occur when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or the status field of that server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
File Download Failed.	User or User group does not have read/write permission for server.xml in device.	Provide read/write permission for user in device

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
XML Parsing Failure	FileName provided might not be a valid XML file.	Ensure the provided filename is a valid XML file.
File Download Failed.	server.xml is not found in the specified directory.	Ensure server.xml is present in the conf directory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
File Not Found	server.xml is not present in the specified directory.	Ensure server.xml is present in the conf directory.
	SSL certificate or key file parsed from configuration file is not present in the specified directory.	Ensure parsed certificate or key file is present in the directory specified in server.xml
JKS Parsing Failure	Password for Keystore file may not be present in server.xml	Password given in server.xml might be incorrect.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Push failed.	Creating local certificate files failed while Backup.	Provide required access to AppViewX to create local files
Certificate Push Failure	Invalid certificate, key, or trust location is given.	Provide the valid certificate, key, or trust location while adding an application connector.
Bind Failed as the SSL is disabled for the port	SSL is disabled for the given port on the server.	Kindly enable SSL for the port on the server.
KeyStore creation failed	Unable to create the Keystore locally.	Provide required access to AppViewX to create local files

Automating CLM for Tomcat (Windows)

Tomcat on Microsoft Windows Servers is an excellent option for organizations utilizing a Windows-based infrastructure, providing strong application server capabilities with seamless integration into the Microsoft ecosystem. It works well with Windows services such as Active Directory and SQL Server, delivering a reliable platform for enterprise applications. While Tomcat was originally designed for Unix-like systems, it is fully compatible with Windows and performs efficiently in this environment. Windows offers a graphical user interface for managing Tomcat, making it easy for administrators accustomed to Microsoft tools. This setup is often used for deploying Java applications that need integration with other Windows services.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

- The Tomcat server must be in the running state. This can be validated by checking services in Windows Task Manager.
- Ensure that the target Hostname is accessible from the Windows Gateway Agent.
- The user must have the necessary permissions to access, download, and upload the **server.xml** and the certificate files associated with the configured settings. (Read and Download permissions should be granted to the user as configured.)
- The directory path containing the **server.xml** file must be specified as the **Installation Directory** during device onboarding.
- Users can manage the Tomcat installed on any drive; however, the account used to manage Tomcat in AppViewX must be configured as a **local administrator** and must have access to both the **Installation Directory** and the **server**.
- Tomcat must be present in the specified directory path, where at least one folder name should include Tomcat.
- To perform certificate discovery, SSL must be enabled on the connector for the respective service. `SSLEnabled="true"` ensures that the connector supports SSL, which is required for certificate discovery.
- Certificates located in paths without the required user permissions cannot be identified. Ensure that the certificates are either configured in the configuration files using accessible paths or update the file permissions to allow the user to access them.
- The system supports **Tomcat**, **ADManager**, and **AD Self Service Plus**. Profiles are automatically created based on the respective installation paths. During the push operation, use the **Device Selection** dropdown to choose the service and view the profiles created for it.

Onboarding Tomcat (Windows) Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Apache Microsoft** from the Vendors list.
5. In the **Server details** section, enter the details as follows.

Server Details - Field Description Table

Field	Description
***Server Type**	Select the **Tomcat** radio button.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Server name**	Enter the name of the designated Apache Tomcat server.
***Hostname**	Enter the hostname of the Apache Server.
Data center	Choose the desired data center. It holds all the SSL related information that is to be retrieved from the Apache server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Apache server. Gateway is the preferred communication mode.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Apache (Tomcat) server device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Field	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Field	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount (when the communication mode is SSM) • All supported external vaults **Note:** • Credential Type does not suppot ssh based authentication for Microsoft devices. • If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. Enter the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Field	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Prerequisites for using the Integrated Windows Gateway mode **Note:** The integrated gateway functionality is not compatible with the following features: • Server addition using the **import** feature • Endpoint CSR generation
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI. **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • **Remote** **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. From the following options, select the gateway: • New • Existing
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

8. In the **Certificate details** section, enter the details as indicated below.

Certificate Details - Field Description Table

Field	Description
Server path	Enter the directory/path where the application is installed. Tomcat ADManager & Self Service Plus has to be integrated under Windows Tomcat, so the paths can be defined as follows: • C:\<parent_folder> e.g. C:\ProgramFiles - Certificates will be discovered from Tomcat, ADManager & Self Service. • C:\ProgramFiles\Apache-Tomcat-8.5.35 - Certificates will be discovered only from Tomcat. • C:\ProgramFiles\ManageEngine\ADManager - here the certificates will be discovered only from ADManager. • C:\ProgramFiles\ManageEngine\ADSelfService - here the certificates will be discovered only from ADSelfService

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

9. Click **Add.**
   Once the server is added successfully, the path will be listed in the table.
10. *[Optional]* Click the (**Delete**) icon, if you want to delete the server path from the list.
11. Click **Save**.
    The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the Status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Onboarding Certificates for Tomcat Windows Server

Discovering Certificates for Tomcat Windows

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to the Tomcat Windows Server

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Tomcat Windows

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Windows Tomcat**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available Windows Tomcat devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, in the **Server selection** section, from the dropdown list in **Available Devices**, select one of the following:
   - **Tomcat**: This selection displays device profiles for Tomcat. The server.xml files are updated based on the profile and the inputs selected/entered in the rest of the fields.

     The profile names use the following naming convention: **WIN_DEVICE :: Tomcat: 8443 : localhost:localhost**
   - **Default**: This selection displays the push-only profiles. The bind operation is not supported.

     The profile names use the following naming convention: **WIN_DEVICE :: Default:**
   - **ADManager**: This selection displays device profiles for ADManager. The server.xml files are updated based on the profile and the inputs selected/entered in the rest of the fields.

     The profile names use the following naming convention: **WIN_DEVICE :: ADManager: 8443 : localhost:localhost**
   - **ADSelfService**: This selection displays device profiles for ADSelfService. The server.xml files are updated based on the profile and the inputs selected/entered in the rest of the fields.

     The profile names use the following naming convention: **WIN_DEVICE :: ADSelfService: 8443 : localhost:localhost**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Profiles are displayed based on the selection made. The **Selected devices** list is updated automatically.

4. From the profiles displayed, to select the required profiles, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled, the existing **server.xml** file is used to create the application connector. If this option is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled).
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate directory**	Enter the path to the location on your local system where the certificate file (to be pushed to the server) is stored.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key directory**	The private key associated with a certificate is stored in a key file. In the **Key directory** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***Key File Name**	Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***KeyStore Location**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)/PKCS#12 (*.p12)/PKCS#12 (*.pfx)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore File Name**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)**. Enter the file name of the keystore file that contains the private keys and the associated certificates. The extension **.key** is automatically populated.
***Password**	This field is displayed when **Certificate Type** = **Default JKS (*.jks)/PKCS#12 (*.p12)/PKCS#12 (*.pfx)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
Alias Name	This field is displayed when **Certificate Type** = **Default JKS (*.jks)/PKCS#12 (*.p12)/PKCS#12 (*.pfx)**. Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Service Restart	To restart the Windows Tomcat service immediately after the certificate is pushed, enable this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***CA File Name**	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the root certificate.
Intermediate File or Bundle Name	This field is displayed when **Push Root and Intermediate Certificates** is enabled. Enter the file name of the intermediate certificate.
***Truststore Location**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. For JKS certificates, the root and intermediate certificates are stored in a truststore file.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the JKS certificate to be pushed, is stored.
***Truststore Password**	This field is displayed when **Certificate Type** = **JKS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the password required to access the truststore file for the JKS certificate to be pushed.
***Truststore File Name**	This field is displayed when **Certificate Type** = **Default KS (*.jks)** and **Push Root and Intermediate Certificates** is enabled. Enter the name of the truststore file for the JKS certificate to be pushed.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.

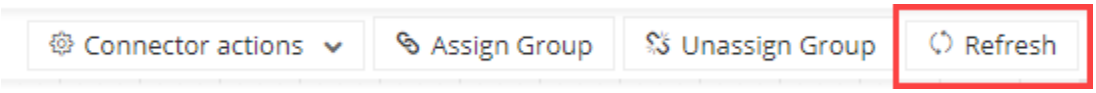
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

d. Click **Update**.

2. To enable auto renewal for the certificate connector:

a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
The **Server Certificate** inventory is displayed.

b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
The holistic view of the selected certificate is displayed.

c. For an existing CA connector for the certificate, hover over .

d. From the menu displayed, click **Edit**.
The certificate details are displayed.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Microsoft Tomcat

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Microsoft Tomcat server.

Issues in Microsoft Tomcat Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Tomcat Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct details and click Save.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Parsing for PTPLD178 completed. 0 ports parsed.	Invalid Tomcat Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page
Error on fetching Tomcat instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C:\tmp_1615504487924.tmp' because it does not exist.	Invalid Server path	Login manually into the windows server and find the Tomcat installation directory path and provide the same path in Server path attribute of tomcat device addition page

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the avx environment. 2. user might not have permission to read in the given source location 3.Device communication might not be established when service has started.	1.Check whether someone deleted the file from AppViewX environment. 2. Verify if read permission is given for the location. 3.Verify the device connection and restart the service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Verify the input details and check for device status error messages in the Issues in Communicating to Tomcat Server section.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e. in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/ write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	"Private key in Device" is enabled in application connector and also private key is available in the certificate	Ensure "Private key in Device" attribute in application connector is unchecked.
PrivateKey in device push invalid	"Private key in Device" is enabled in application connector, but key is not available in device.	Ensure to enable "Private key in Device" attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Automating CLM for JBoss

JBOSS can be configured on two types of machines: Linux and Windows. Developed by JBOSS, this server can be deployed on both operating systems, providing flexibility and compatibility for various environments.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

- Ensure that the following packages are installed to facilitate device addition for linux:
  - sudo/dzdo (optional, as per the access elevation selected)
  - timeout
  - base64
- Ensure that the target IP address is accessible from the cloud connector and the port is open.
- Make sure that the language setting for the JBoss Server is set to English. Ensure that the sudo prompt string follows the standard Linux format, which is typically "[sudo] password for <your_username>:"
- Only certifiticates in .pem, .crt, and .cer formats and key files are discovered.
- SSH private keys cannot be used in conjunction with password-enabled sudo/dzdo settings. Therefore, if an SSH key is used for authentication, ensure that the sudo/dzdo configuration is set to passwordless.
- Certificates are not identified from the path that does not have the required permission such as 640 for the user. Ensure that the file is the same as configured in device addition; hence, configure the certificates in the config files with accessible path or change file permissions to make the files accessible.
- Verify that the commands needing sudo or dzdo access have been enabled on the server.
- Check for the ServerRoot location in the **httpd** file. Make sure it holds forward slashes(/) as path separator as in other Linux-based file locations. (This might lead to failure in managing JBoss server installed on the Windows machines).

Onboarding JBoss Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **JBoss** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Operating system type**	Select the **Linux** radio button.
***Server name**	Enter the name of the designated JBoss Linux server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the JBoss server.
Communication mode	Select the SSH or SSM protocol to be used for communication between the AppViewX node and the JBoss server. **SSH** is the preferred communication mode.
***IP address/ FQDN**	Enter the IP address or the fully qualified domain name (FQDN) of the server that is to be onboarded.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the JBoss server device.
   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx • *SSH*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If SSH is selected, enter the ***Username**, ***Upload key** file, and enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If **Communication mode** = **SSH** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	By default, application uses none. You can change the command if needed. **Note:** SSH key-based authentication doesn't support password enabled sudo/dzdo.

If **Communication mode** = **SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. Click **Save**.
   The JBoss Linux device is onboarded successfully.

Onboarding JBoss Windows

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **JBoss** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Operating system type**	Select the **Windows** radio button.
***Server name**	Enter the name of the designated JBoss Windows server.
***Hostname**	Enter the hostname of the windows server that is to be onboarded.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the JBoss server. **Gateway** is the preferred communication mode.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the JBoss server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the JBoss server device.

   If **Communication mode** = **SSH** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - Appviewx **Note:** If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry and SSH)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
**: Mandatory fields*	

7. In the **Vendor Specific Details** section, select/enter the details as indicated below.
   If the **Communication mode = Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\JBoss-Tomcat-8.5.35
**: Mandatory fields*	

If the **Communication mode = SSM** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Installation directory path**	Enter the directory/path where the application is installed. *Example*: C:\Tomcat8\JBoss-Tomcat-8.5.35
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Example: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

8. In the **Windows gateway details** section, enter the details as indicated below. (This section is not displayed if **Communication mode = SSM**)

Windows Gateway Details - Field Description Table

Fields	Description
***Gateway type**	Select to use the *PowerShell* or *WMI* commands as the gateway communication mode.
***Gateway location**	The value Remote is selected by default.
***Select gateway**	Select the *New* or *Existing* gateway to be used. The below fields are enabled/ disabled according to the selection.
***Windows gateway name**	Enter the new gateway name. (Enabled when *New* is selected as gateway)
***Windows gateway URL**	Enter the URL for the new gateway. (Enabled when *New* is selected as gateway)
Client authentication certificate	Click Browse and upload the client authentication certificate for the new gateway. (Enabled when *New* is selected as gateway)
***Windows gateway**	Select any of the existing configured gateways from the dropdown list. (Enabled when *Existing* is selected as gateway)
**: Mandatory fields*	

9. Click **Save**.

   The JBoss Windows device is onboarded successfully.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified status in the status column.
   The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Discovering Certificates for JBoss

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding and Pushing Certificates to JBoss Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for JBoss

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **JBoss**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available JBoss devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Use Existing Configuration	If the **Use Existing Configuration** option is enabled,the existing **server.xml** file is used to create the application connector. (By default, this option is selected.) If it is disabled, the server configuration XML file will be overwritten with the values specified in the fields below (displayed only if this option is disabled). **Note:** After discovery, on editing the application connector, the use existing checkbox will be the selected/enabled state
Certificate Type	This field is displayed when **Use Existing Configuration** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the file type of the certificate to be pushed.
***KeyStore Location**	This field is displayed when **Use Existing Configuration** is enabled and **Certificate Type** = **JKS (*.jks)**. For JKS certificates, a keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the JKS keystore file, for the certificate to be pushed, is stored.
***Password**	This field is displayed when **Use Existing Configuration** is disabled and **Certificate Type** = **JKS (*.jks)**. Enter the password required to access the keystore file for the JKS certificate to be pushed.
***Alias Name**	This field is displayed when **Use Existing Configuration** is disabled and **Certificate Type** = **Default JKS (*.jks)** or **JKS (*.jks)**. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The certificate topology view is displayed.

3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

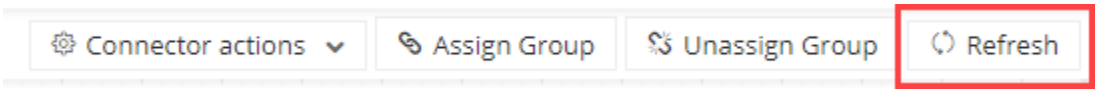
The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.
   The holistic view of the selected certificate is displayed.

   Note: For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
    a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
    The **Group** page is displayed.
    b. From the **Name** field, select the required certificate group.
    The **Group : Modify : <group name>** page is displayed.
    c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
    d. Click **Update**.
2. To enable auto push for the certificate connector:
    a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
    To add an application connector, follow the instructions given here.
    b. From the menu displayed, click **Edit**.
    The **Edit Application Connector** pop-up is displayed.
    c. Select the **Push automatically** checkbox.

    > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

    d. Click **Save**.
    The holistic view of the selected certificate is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

Note: An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Troubleshooting Linux JBoss Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities.This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Linux JBoss server.

Issues in Linux JBoss Server Addition using AppViewX UI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Linux JBoss Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is either null or empty.	Provide device name as it is a mandatory field.
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Device IP/FQDN cannot be null or empty.	Device IP/FQDN is empty.	Provide device IP/FQDN as it is a mandatory field.
Invalid device IP/FQDN address.	IP/FQDN address is not valid.	Provide valid IP/FQDN address.
Communication to <ip/fqdn> has failed. Caused by: java.io.IOException: Unable to authenticate with password, keyboard-interactive and publickey methods Possible Remediations: 1. Kindly check the credentials provided.	Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct password and click Save.
Communication to <ip/fqdn> has failed. Caused by: java.net.SocketException: Network is unreachable (connect failed)	IP/FQDN provided is not reachable	Check manually by establishing an SSH session to the target device with the provided IP/FQDN.
Communication to <IP/FQDN> has failed. Caused by: java.net.ConnectException: Connection refused (Connection refused) Possible Remediations: 1. Kindly check the SSH Port configurations. 2. Kindly check the firewall settings	Problem with port configuration	Check if the configured port in the device addition page is correct.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed. Caused by: java.io.IOException: Key exchange was not finished, connection is closed.	Problem with SSH key handshake	Request to check the ciphers, key and HMACs configured in the target device and ensure AppViewX SSH-plugin supports the same
<IP/FQDN> has 0 JBoss instance(s)	No JBoss server running in the target device,	Login via SSH to the target device and execute the below command to check the status of the JBoss server “ps -ef | grep jboss”.

Issues in Accessing the Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Sudo Access failure	Linux Commands execution with sudo fails.	Verify if the system has the correct sudo setup.
dzdo Access failure	Linux Commands execution with dzdo fails.	Verify if the system has the correct dzdo setup.
Permission denied for file/ location.	File might not be present in the avx environment. User might not have permission to read in the given source location.	Check whether someone deleted the file from AppViewX environment. Verify if read permission is given for the location. Verify the device connection and restart the service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Device communication might not be established when service has started.	

Issues in Credential List

Error Message	Possible Cause	Possible Solution
Invalid details	Mandatory credential details are missing.	Provide all the mandatory details to store the credential.
credentials already exist.	Credential List with the same name already exists.	Provide a unique name to each credential list.
Invalid file format. Accepted formats are .pem and .txt	The Identity Key file uploaded is not having the correct format.	Provide key file with correct format (.pem or .txt)

Issues in Managed Server

Error Message	Possible Cause	Possible Solution
The selected devices are managed. The operation cannot be performed.	Device cannot be managed because it is already in the managed state.	Unmanage the device(s) in the managed state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Unmanaged Server

Error Message	Possible Cause	Possible Solution
The selected devices are already unmanaged. The operation cannot be performed.	Device cannot be unmanaged because it is already in the unmanaged state.	Manage the device(s) in an unmanaged state before performing action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Fetch config not allowed for Unmanaged devices	Fetch config operation is only allowed on the devices which are in managed state.	Manage the device(s) in an unmanaged/in-progress state before performing action.
Device with inprogress status cannot be updated	Update action cannot be performed on a device in an in-progress state.	Wait for the device to be resolved to a state before performing action.

Issues in Import Server

Error Message	Possible Cause	Possible Solution
Invalid file type. Please select a valid file format (csv / xlsx / xls).	File type uploaded is not in expected format.	Supported file types are CSV/Xls/xlsx only. Check for the extension of the uploaded file.
Maximum five files allowed, please delete any completed file.	Maximum of 5 files can be maintained in file history of import page.	Delete any of the parsed/completed files to upload a new one.

Issues in Export Server

Error Message	Possible Cause	Possible Solution
Exception while exporting	General failure - Unable to create file on the local system due to permission issue. Unable to fetch device list from the database.	Provide access to be able to create the file on the local system. (e.g. check the directory where it is trying to export and give access to AppViewX for that directory) Make sure the database is running and has correct data.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <IP/FQDN> has failed.	Device communication has failed due to invalid credentials / SSH Port	Verify the input details and check device status error messages in the Issues in Communicating to Linux JBoss Server section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have the required permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct “connectorId” if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/write access to the path configured in application connector to certificate push.
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR generate option from Device.

Troubleshooting Windows JBoss Server

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. Effective troubleshooting documents depend on the availability of useful, detailed information. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback, and other actions associated with Windows JBoss server.

Issues in Windows JBoss Server Addition using AppViewX GUI

Error Message	Possible Cause	Possible Solution
Device Name already exists.	A device with the same name already exists in inventory.	Check the Device name, it should be unique.
Details incorrect	Some of the mandatory fields might be missing or might be invalid.	Add all the valid information in the mandatory section.

Issues in Communicating to Windows JBoss Server

Error Message	Possible Cause	Possible Solution
Device name cannot be null or empty.	Device name is empty.	Provide device name as it is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Invalid device name.	Device Name is not valid.	The Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Click on the device name in the Inventory Page. Update the correct details and click Save.
Communication to <Hostname> has failed due to Error while communicating via windows agent service	Windows agent provided is not reachable	Check Windows agent is Up and running and update the valid agent in the device addition page.
Error on fetching JBoss instance, config fetch process failed due to No configuration file found. Check installation directory path.	Provided installation directory path does not have JBoss configuration files like server.xml / standalone.xml	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.
Error on fetching JBoss instance, config fetch process failed due to df9cbf67-e1af-4d8c-8a7c-fe88bb83e0b3: PowerShell ScriptExecution Error in PTPLD178 : Cannot find path 'C: \tmp_1615504487924.tmp' because it does not exist.	Invalid installation directory path	Login manually into the windows server and find the installation directory path which has the JBoss configuration files (server.xml or standalone.xml) and provide the same directory path in JBoss device addition page.
JBoss version fetch is failed	No JBoss server running in the target device / something wrong in the JBoss installation	Login manually into the windows server and find the JBoss server bin directory and run the below command to validate the JBoss version

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution

		For JBoss 4.0.5
		`<JBoss_server_Directory>/bin/run.bat -V`
		For JBoss 6.4 and 7.0
		`<JBoss_server_Directory>/bin/standalone.bat -V`
		Currently only JBoss 4.0.5, 6.4 and 7.0 versions are supported in AppViewX.

Issues in Accessing Server

Access Issues might be reproduced when communicating with servers while discovering or fetching configuration files. These errors can be collected either from logs, API responses, or in the status field for the particular server.

Error Message	Possible Cause	Possible Solution
Permission denied for file/location.	1. File might not be present in the environment. 2. User might not have permission to read in the given source location. 3. Device communication might not be established when service has started.	1. Check whether someone deleted the file from the environment. 2. Verify if read permission is given for the location. 3. Verify the device connection and restart the service.

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Hostname / Username / Password of the device added might be wrong.	Verify the input details and check for device status error messages in the Issues in Communicating to Windows JBoss Server section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in CSR generation

Error Message	Possible Cause	Possible Solution
Problem while generating csr on target server	General Failure - SSH/SFTP communication failure	Provide correct credentials and make sure device communication is successful.
Invalid key type specified in the request	Given key type might not be supported by open SSL in the target machine.	Provide valid key type.
Problem while generating csr on the target server.	Location might not have permission.	Check the permission and provide it.
CSR and Private key has been failed	Open SSL configuration might be wrong in the target machine.	Check and correct open SSL configuration in the device.
CSR generation got failed	User has restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is	Push to device after certificate has been retrieved from CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	unavailable, i.e, in a new state.	
Certificate Push failed	User has restricted access to the path configured to push the certificate in the application connector	Kindly ensure the user is configured while device addition has the read/ write access to the path configured in application connector to certificate push.
Certificate push failed due to Private key In device configured. But key content is available with the certificate from appview pushRequest So failing push request.	“Private key in Device” is enabled in application connector and also private key is available in the certificate	Ensure to uncheck “Private key in Device” attribute in application connector
PrivateKey in device push invalid	“Private key in Device” is enabled in application connector, but key is not available in device.	Ensure to enable “Private key in Device” attribute in application connector, if the certificate does not have the key and the certificate is generated using CSR gen option from Device.

Automating CLM for Linux

Onboarding the Linux Server Device

Prerequisites

1. Ensure that SSH users have the required read and write permissions to perform CLM actions on the server device when access elevation is set to "**None**."
   If access elevation is configured as "**sudo**" or "**dzdo**," all commands for CLM operations will be executed using sudo or dzdo.
2. If sudo/dzdo access elevation is enabled on the device onboarding page, ensure that the user has the necessary permissions to execute the sudo command provided below.
3. Ensure that the following packages are installed to facilitate device addition:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- sudo/dzdo (Only applicable if access elevation is selected as sudo/dzdo in the device onboarding page)
- timeout
- base64

4. Ensure that the OpenSSL toolkit on the Linux machine is installed.

> **Note:** This package is essential for supporting endpoint enrollment. However, if endpoint enrollment is not required, the package is optional.

5. Ensure the server's resource health remains above the 50% threshold.
6. Ensure that the target IP address is accessible from the cloud connector and the port is open.

> **Note:** To SSH into a machine using a specific port, you can use the following command:
>
> ```
> ssh -p <port_number> <username>@<hostname_or_ip_address>
> ```

7. Ensure that the SFTP is configured.

> **Note:**
> Avoid restricting SFTP sessions to a single connection, as this may cause failures in push use cases. To prevent such issues, adjust the settings in
>
> `/etc/security/limits.conf`
>
> to allow up to 5 connections.

8. Ensure that GSKit is installed on the server to work with the KDB certificate.
   For the KDB use case, one of the available packages is utilized.

   To verify if the package is installed on the machine, use the following commands:

```
dspmqver -p 64

gsk8capicmd -version | grep FileVersion

gsk8cmd -version | grep FileVersion

gsk7capicmd -version | grep FileVersion

gsk7cmd -version | grep FileVersion
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- The command gsk8capicmd_64 -version will be supported in the future release v2024.2.0.0.
- The first successfully executed command determines the package to be used.

9. To discover a password-protected certificate, ensure the password is added to the password vault at **CERT+** > **ADMINISTRATION** > **Password Vault**.
10. SSH private keys are incompatible with password-enabled sudo/dzdo settings. Therefore, when using an SSH key for authentication, ensure that sudo/dzdo is configured for passwordless access.
11. Certificates cannot be identified from the mounted paths /boot, /bin, /dev, /lib, and /sbin. It is recommended to move the certificate to an alternative location.
12. Host-level configurations take precedence over global settings, allowing you to override global settings at the host level.

Note: The global setting can be configured in the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **(Device Settings)**.

13. Port scanning is disabled by default during Linux discovery. However, configurations are enabled at both the host level and global level to control this feature.
14. If device onboarding fails due to host key algorithm mismatches, activate the required algorithms on the client or server. Add deprecated algorithms only if necessary.
15. It is recommended to exclude the NAS mount paths from certificate scanning which might consume additional resources during scanning and might affect the server performance.

Onboarding Linux

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
4. Select the **Linux** logo from the Vendors list.
5. In the **Server Details** section, enter details as mentioned below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter a unique name for the designated Linux server that is to be onboarded
***IP address/ FQDN**	Enter the valid IP address or fully qualified domain name (FQDN) for device communication and integration with the Linux server.
Data center	Choose the desired data center.
Communication mode	Select the *SSH* or *SSM* protocol to be used for communication between the AppViewX node and the Linux server. **SSH** is the preferred communication mode.
***SSH Port**	Retain the value 22; it is the default port used for the SSH communication mode. (The field is not displayed for SSM communication mode.)
Cert sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as follows.

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *Credential List - HashiCorp* • *SSH*

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: • All other vault settings (BeyondTrust, Cyberark, Hashicorp Vault, Thycotic, and so on.) configured in the **Credentials** will be displayed in the dropdown. • If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values. • If **Credential list - HashiCorp** is selected, the ***Credentials list** dropdown field is displayed with credential type by default. • If SSH is selected, enter the ***Username**, ***Upload key** file, and optionally enter the **Passphrase** for authentication.
***Username**	Enter the designated username for authentication. **Note:** This field appears when the credential type is selected as Manual entry or SSH.
***Password**	Enter the secure password. **Note:** This field appears when the credential type is selected as Manual entry.
**: Mandatory fields*	

7. In the **Service account credentials** section, select/enter the details as indicated below. If interactive mode is not enabled for the service account on the Linux machine, the configured service account will switch the session from the logged-in SSH account to the service account using the command: `su - {serviceUserName}`. Once the session is switched, all subsequent commands will execute within the context of the service account session.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Service account credentials - Field description table

Fields	Description
Username	Enter the designated username for authentication. **Note:** The service account is not used for authentication; instead, it is used to switch the session from the logged-in SSH user account to the service account.
Password	Enter the secure password.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, enter details as mentioned below.

Vendor Specific Details - Field Description Table

Fields	Description
Access Elevation	Select from the following:. • *None* (default) • *sudo*- to execute with root privileges using sudo access • *dzdo*- to execute with root privileges using dzdo access. **Note:** SSH key-based authentication does not support password-enabled sudo/dzdo.
Discover Formats	The Discover Formats fields contain all the possible certificate formats that are applicable to the 'Default' scan type. The formats include KBD(*.kbd), PEM(*.crt), PEM(*.cer), PEM(*.pem), DER(*.der) DER(*.cer), PKCS#7(*.p7b), PKCS#7(*.p7c), PKCS#12(*.p12), PKCS#12(*.pfx), JKS(*.JKS), JKS(*.keystore). To delete the certificate format from the scan, click the 'x' icon in the respective cert type. To delete all the certificate formats from the scan, click 'Clear' on the top-right of the field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
File Upload Temp Path	This field is displayed if the Access elevation value is selected as sudo or dzdo. Enter the path of the temp folder *Example*: /cert/temp This field is applicable for Push and CSR generation operations. This directory must have common access (RW) for the logged-in user and the service admin user if Service Account credentials are entered.
Enable access elevation for the service account?	When enabled, the commands are executed with selected access elevation. **Note:** • By default, this field is disabled. • This field is enabled only for a service account user when an Access Elevation type, such as sudo or dzdo, is selected.
Enable Network Scan	Select the checkbox to perform a network scan in addition to the managed device discovery scan for these devices. **Note:** • By default, this field is disabled and can be enabled through a global device setting. [**CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **(Device Settings)]**
**: Mandatory fields*	

9. In the **Certificate details** section, enter the details as indicated below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
Certificate Directory	Enter the actual directory/path where certificates are stored in the Linux server. *Example*: /cert/files
Scan Type	Select any of the following: • *Default* - System scans for all certificate formats and adds them in the certificate inventory. **Note:** It scans the provided directory and subdirectory as well. • *Aggressive* - System scans for all keystore files with non-standard SSL extensions and also scans for trust certificates from extension less files. **Note:** It scans only the given directory.
***Operation**	Select the value *include* or *exclude* from the dropdown field. It indicates that the specified certificate directory will be included/excluded from the certificate scan process.
**: Mandatory fields*	

10. Click **Add**.
    The certificate location will be listed in the table.
11. *(optional step)* Click the (Delete) icon if you want to delete the certificate details from the list.
12. Click **Save**.
    The Linux device is added successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The **Server Inventory** page is displayed.
3. Check that the device name appears in the inventory (name column) with the specified Status column.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The status column will have the value Managed/Monitored/Ignored if the connection is successful or displays Failed/Unresolved in case of failure.

4. From the Status column, click the Managed/Monitored/Ignored/Failed/Unresolved.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Discovering Certificates for Linux

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding and Pushing Certificates to Linux Device

Important: Refer to the pre- and post-push script usage instructions here.

Linux Server

Important: If the certificate is generated with CSR generation at endpoint, if an application connector is created for the certificate, the following fields will be auto-populated/selected and cannot be modified:

- **Category**
- **Vendor**
- **Key Location**
- **Private key in Device**

Additionally, the available profiles will be filtered for the device profile selected at the time of certificate enrollment here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the client (or) server certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **LinuxServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Linux Server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .

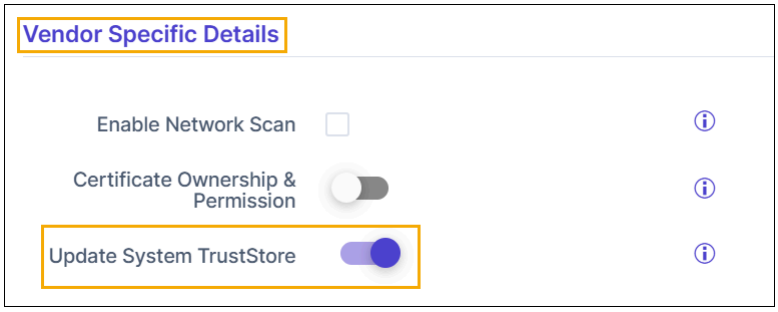
You can use the **Available Devices** dropdown list to filter devices based on functionality.

The **Selected devices** list is updated automatically.

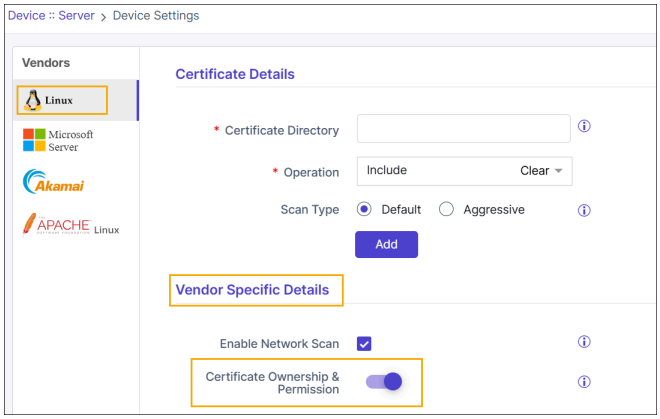
4. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Enable Truststore Update	This field is displayed for all **PEM** certificate types. Click the radio button to enable the Update System TrustStore option for root and intermediate certificates. **Note:** By default, this option is disabled. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** <⚙> **Vendor Specific Details** section > **Update System TrustStore**. 
Certificate Ownership & Permission	Enable the toggle button to customize the certificate ownership and define the file permissions for the certificates. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** <⚙> **Vendor Specific Details** section > **Certificate Ownership & Permission**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	 Field descriptions for the Certificate Ownership & Permission Details
Custom Push	This field is displayed for all **PEM** and **DER** certificate types. From the following options, select the method of pushing certificates: • **Chain**: The full certificate chain, which includes the end, intermediate, and root certificates, will be pushed to the server. • **Issuer & Server**: The server's certificate and its issuer's certificates will be pushed to the server. • **Server Only**: Only the server's certificate will be pushed to the server.
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Linux Server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Certificate Location	This field is displayed for all PEM, DER and PKCS#7 certificates. Enter the path to the location on your local system where the certificate file to be pushed is stored.
Key Location	This field is displayed for all PEM, DER and PKCS#7 certificates. The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***KeyStore Location**	This field is displayed for the PKCS#12 and JKS certificates. A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the keystore file, for the certificate to be pushed, is stored.
***KeyStore Password**	This field is displayed for the PKCS#12 and JKS certificates. Enter the password required to access the keystore file for the certificate to be pushed.
***Alias Name**	This field is displayed for the PKCS#12 and JKS certificates. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Truststore Location	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the certificates to be pushed, is stored. **Note:** Truststore Location can be specified without the file extension as well.
Truststore password	This field is displayed for the JKS certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

Field descriptions for the Certificate Ownership & Permission Details

Field	Description
Owner	Enter the username for certificate ownership on the target device.
Owner Permission	Select the owner permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
User Group	Enter name of the user group that requires access to the certificate.
User Group Permission	Select the group permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
Other User Permission	Select the other user permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Pushing a Server Certificate to a Device

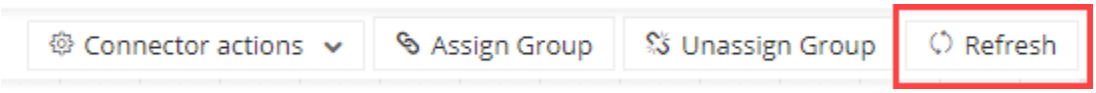
1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.
   d. Click **Update**.
2. To enable auto renewal for the certificate connector:
   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.
   c. For an existing CA connector for the certificate, hover over ⋯.
   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.
   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.
   c. Select the **Push automatically** checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.

The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Automating CLM for Windows Environment

Setting up AppViewX Windows Gateway

AppViewX Windows Gateway

The AppViewX Windows Gateway is packaged with two components:

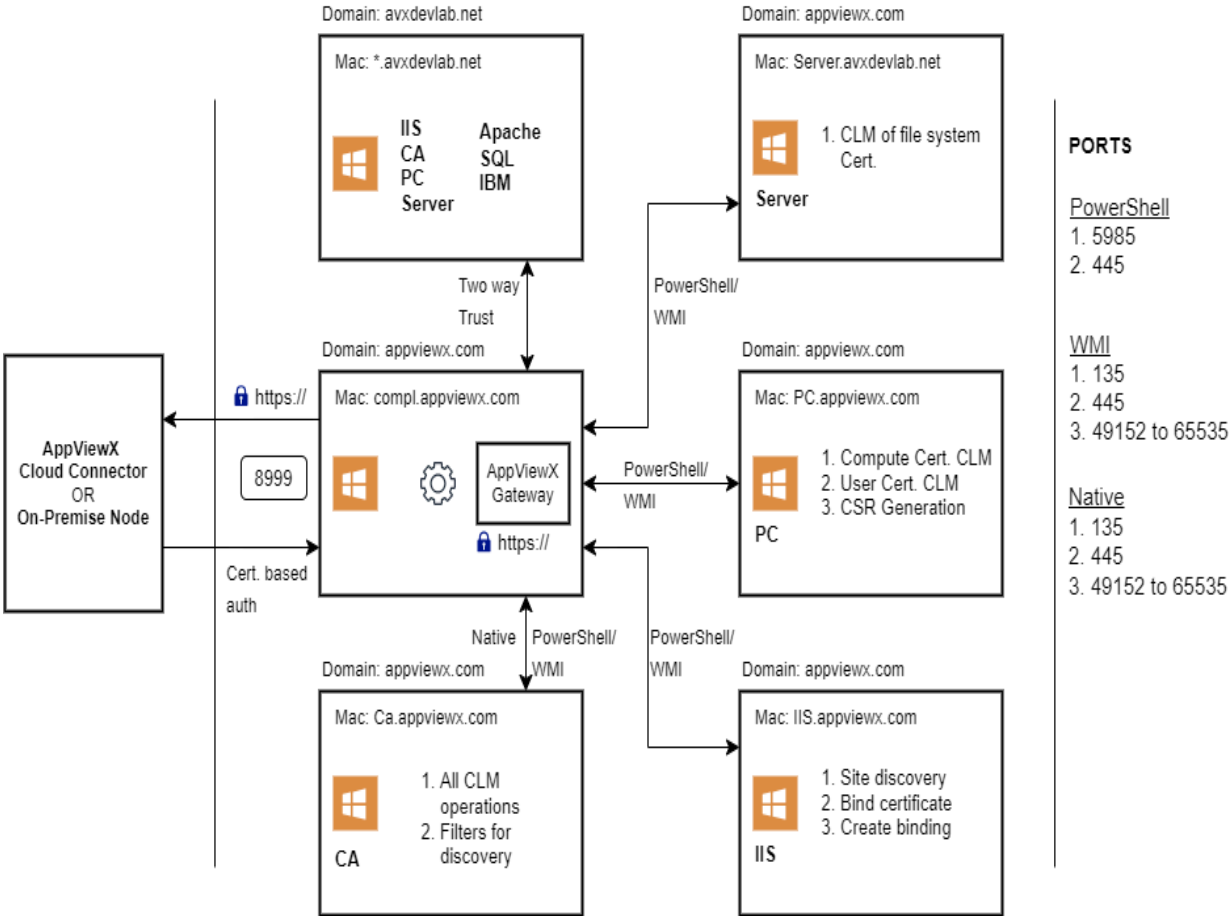
- AppViewX Windows Gateway Service
- AppViewX Windows Gateway Troubleshooting tool

AppViewX Windows Gateway service is a Windows Communication Foundation service that enables secure communication between AppViewX and Windows server infrastructure. Following are the key features of the that are supported by AppViewX for Windows Server Infrastructure:

- Certificate Life Cycle Management (CLM) on Windows servers (version 2012 R2 and above), Microsoft CA Servers, IBM Websphere, and Weblogic.
- Binding of certificates to IIS (Version 7.5 and above)
- Discovering certificates from the file system
- Executing custom scripts on PowerShell

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AppViewX Windows Gateway Troubleshooting tool facilitates the trouble shooting of any issues in the communication between AppViewX Windows Gateway service and the Windows server infrastructure in your premises.



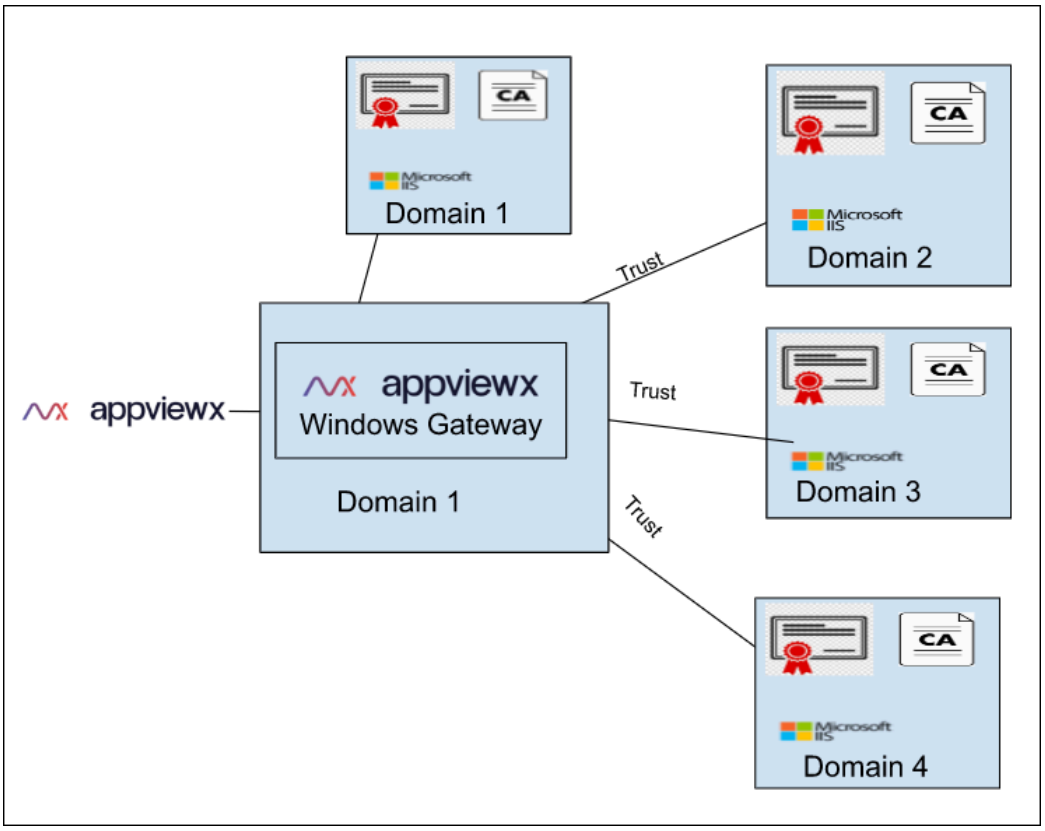
Deployment Modes

AppViewX WG installation is different for trusted and untrusted domains.

Trusted Domains

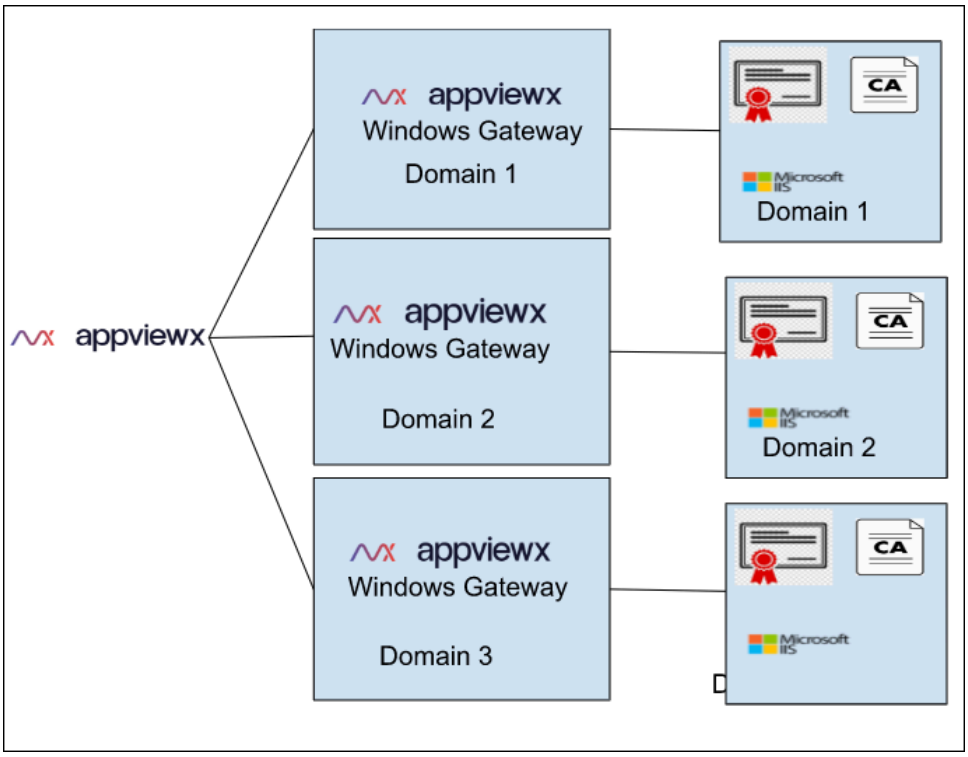
If your organization has multiple domains and each of these domains are trusted, then as depicted in the following figure, one installation of the AWG would be sufficient to manage the Windows server infrastructure of all the domains.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Alternatively, if the domains are independent, then at least one installation of the AWG is needed for each such untrusted domain, as shown in the figure below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Setting up the AppViewX Windows Gateway

Step 1: Checking Prerequisites

Software prerequisites

Name	Description
Operating System	AppViewX Windows Gateway is supported Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022.
.NET framework	.NET framework version 4.5.2 is required.
Admin access	Administrator privilege is needed to install AppViewX Windows Gateway.
PowerShell	PowerShell version 4.0 is needed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Hardware prerequisites

Hardware	Capability
RAM	8 GB
HDD	10 GB
CPU	Intel or AMD processor with 64-bit support, 1.8 GHz or faster processor

Firewall prerequisites

Component	Port
Default Port communication from AppViewX to a AppViewX Windows Gateway	8999

Note:

- The firewall must not block the following port and the respective port must open on the Agent.
- During the installation of AppViewX Windows Gateway, the default port can be reconfigured. For more details refer Step 3 of the installation process.

Step 2: Downloading the AppViewX Windows Gateway Installer

Download and unarchive the **AppViewX.CertPlus.Installer.zip** file from the release portal, under the latest version of AppViewX, in the **Additional Resources** section. The download package consists of the following files:

File Name	Description
AppViewX.CertPlus.Installer.exe	Installer executable
ClientCertificateGateway.pfx	Default client certificate
ServerCertificateGateway.pfx	Default server certificate
config.xml	Application configuration settings that will override the default settings after the AppViewX Windows Gateway is installed.
Readme.txt	Help file with details of the AppViewX Windows Gateway.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

File Name	Description
InstallationLog.txt	Logs the success and error messages from the installation process.

Step 3: Installing the AppviewX Windows Gateway

Before you begin: By default, the AppViewX Windows Gateway securely communicates with AppViewX using the server/client certificates that are shipped along with the AppViewX Windows Gateway installer. If you choose to use a different server and client certificate for authentication, then follow the steps below:

1. From Windows explorer, browse to the location where you have unarchived the AppViewX Windows Gateway installer package.
2. Rename the default server certificate **ServerCertificateGateway.pfx** to **ServerCertificateGateway-Backup.pfx** and the client certificate file **ClientCertificateGateway.pfx** to **ClientCertificateGateway-Backup.pfx**.
3. Copy the server and client certificates that you intend to use in this directory.
4. Rename the server certificate file to **ServerCertificateGateway.pfx** and the client certificate file to **ClientCertificateGateway.pfx**, and then replace the default certificates in the installation folder.

Note: While installing the AppViewX Windows Gateway, you will be prompted to provide the server and client passwords.

CAUTION: If the certificate is replaced, ensure that the respective password has been provided to add the certificate to the store. The incorrect password during the installation of AppViewX Windows Gateway will cause the Windows Agent installation to fail.

1. Execute the **AppViewX.CertPlus.Installer.exe** file.
   The welcome screen for the setup wizard is displayed.
2. Click **Next**.
   The **License Agreement** is displayed.
3. Select **I accept the terms in the license agreement**.
4. Click **Next**.
   The **Destination Folder** screen is displayed.
5. To install the AppViewX Windows Gateway at the default location, click **Next**.
   OR

   To change the default destination folder:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Click **Change**.

b. On the **Change Current Destination Folder** screen, use the **Look in** dropdown list/ (up one level) icon/ (create new folder) icon to navigate to/create the required destination folder.

c. On the **Change Current Destination Folder** screen, use the **Look in** dropdown list/ (up one level) icon/ (create new folder) icon to navigate to/create the required destination folder.

d. Click **OK**.

e. On the **Destination Folder** screen, click **Next**.
The **Optionally you can modify the below details** screen is displayed.

f. Enter the details as required.

Field descriptions for the details

Field	Description
Please select default certificate store	Select the certificate store from which the certificates will be discovered and pushed to by AppViewX from the following options: • Current User Store This type of certificate store is local to a user account on a computer. It is located in the registry under the HKEY_CURRENT_USER root. • Local Machine Store (default) This type of certificate store is local to a computer and global to all the user accounts on the computer. It is located in the registry under the HKEY_LOCAL_MACHINE root. This configures the gateway for communicating with the appropriate certificate store.
Port	Port for accessing the service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Default value: 8999 (can be modified if required)
Server certificate thumbprint	If you are using a custom certificate, enter the corresponding server certificate thumbprint value.
Client certificate password	Password for accessing the client certificate For custom client certificates, enter the certificate password.
Server certificate password	Password for accessing the server certificate For custom server certificates, enter the certificate password.

Note: Refer to the **Before you Begin** section to use custom server and client certificates.

6. Click **Next**.
   The **Ready to Install the Program** screen is displayed.
7. Click **Install**.
   This will:
   • Install the AppViewX Windows Gateway Troubleshooter tool
   • AppViewX Windows Gateway service

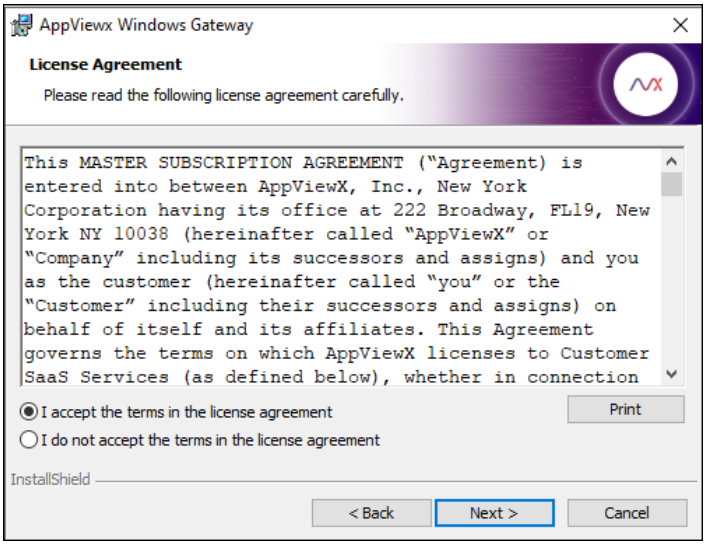
Navigating through the Installation

1. Execute the **AppViewX.CertPlus.Installer.exe** file.
   The following welcome screen for the setup wizard is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Click **Next**.

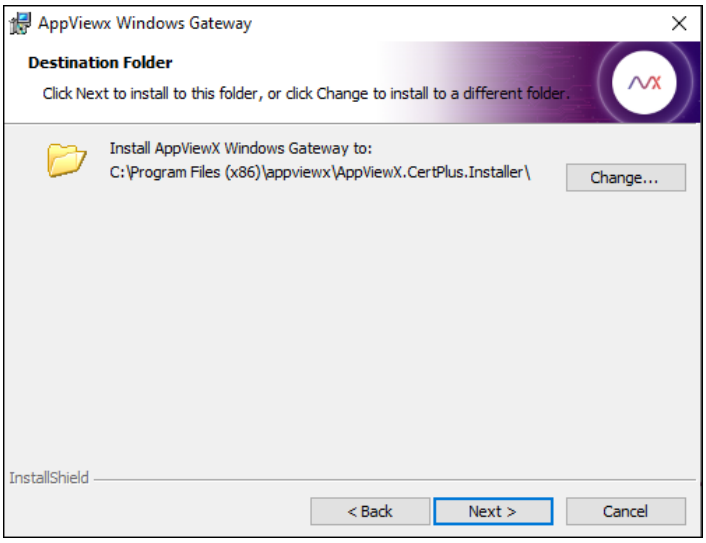
   The **License Agreement** is displayed.



3. Select **I accept the terms in the license agreement**.
4. Click **Next**.

   The **Destination Folder** screen is displayed.

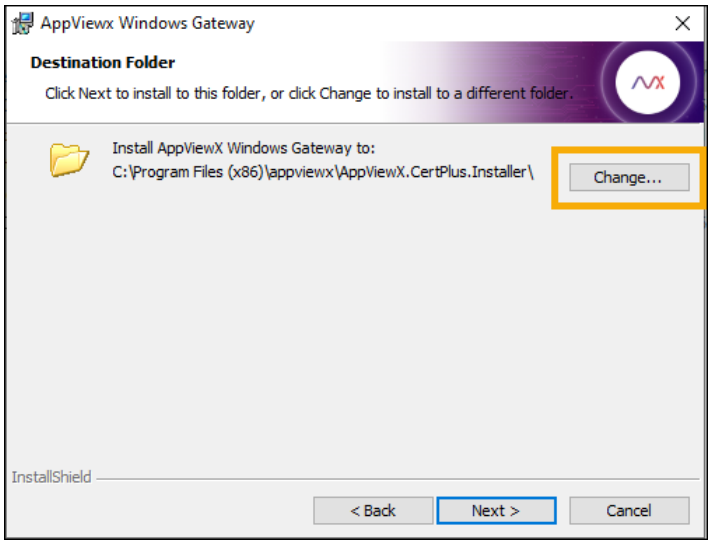
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



5. To install the AppViewX Windows Gateway at the default location, click **Next**.

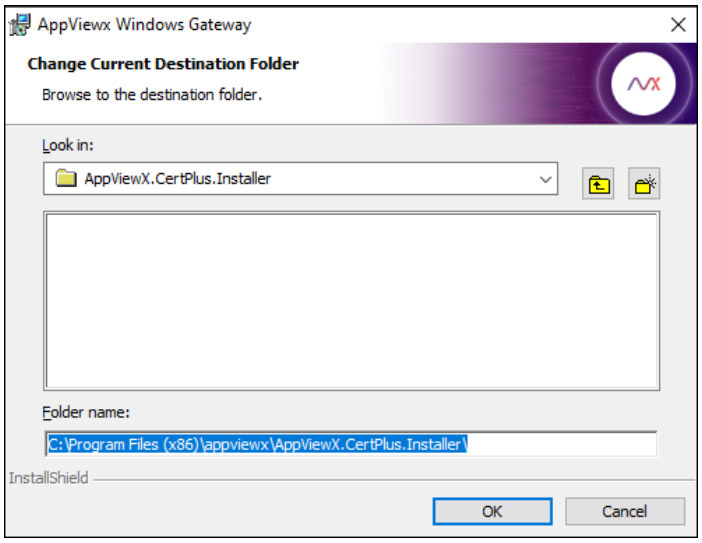
   To change the default destination folder:

   a. Click **Change**.



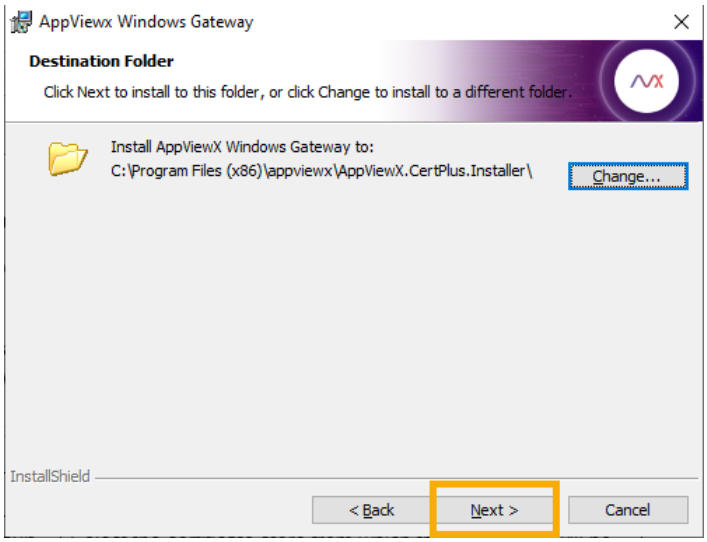
   b. On the **Change Current Destination Folder** screen, use the **Look in** dropdown list/ (up one level) icon/ (create new folder) icon to navigate to/create the required destination folder.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



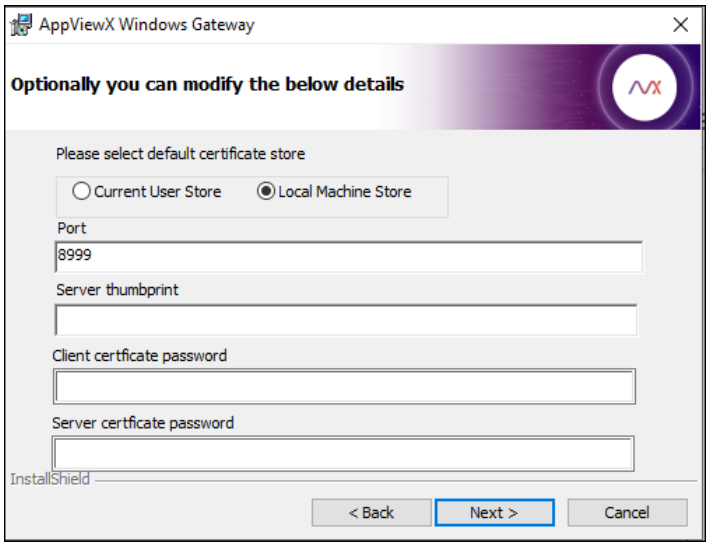
c. Click **OK**.

d. On the **Destination Folder** screen, click **Next**.



The **Optionally you can modify the below details** screen is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Enter the following details (optional):

Field	Description
Please select default certificate store	Select the certificate store from which the certificates will be discovered and pushed to by AppViewX from the following options: • Current User Store This type of certificate store is local to a user account on a computer. It is located in the registry under the HKEY_CURRENT_USER root. • Local Machine Store (default) This type of certificate store is local to a computer and global to all the user accounts on the computer. It is located in the registry under the HKEY_LOCAL_MACHINE root. This configures the gateway for communicating with the appropriate certificate store.
Port	Port for accessing the service.

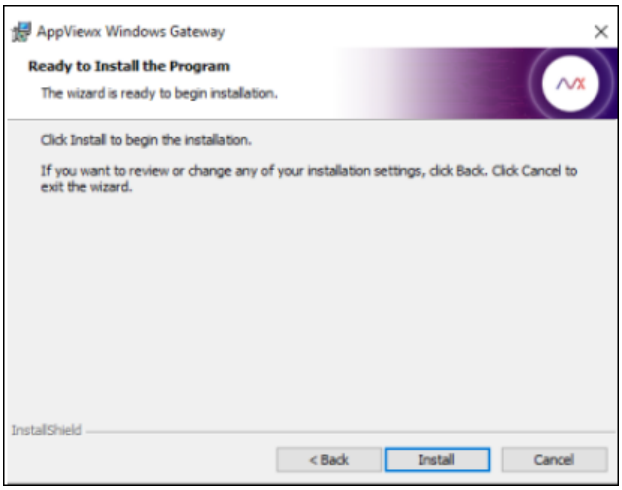
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Default value: 8999 (can be modified if required)
Server certificate thumbprint	If you are using a custom certificate, enter the corresponding server certificate thumbprint value.
Client certificate password	Password for accessing the client certificate For custom client certificates, enter the certificate password.
Server certificate password	Password for accessing the server certificate For custom server certificates, enter the certificate password.

Note: Read the **Before you Begin** section to use custom server and client certificates.

6. Click **Next**.

   The Ready to Install the Program screen is displayed.



7. Click **Install**.

   This will:

   • Install the AppViewX Windows Gateway Troubleshooter tool

   • AppViewX Windows Gateway service.

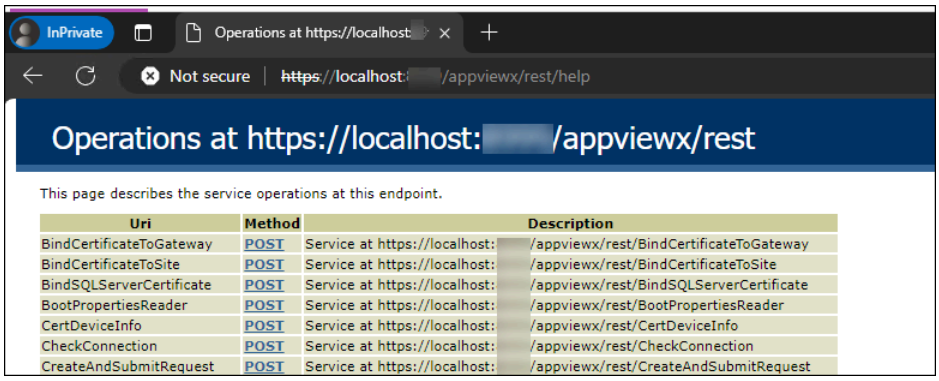
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Step 4: Verifying the AppviewX Windows Gateway Installation

1. Open **Services.msc** and ensure *AppViewXCertPlus* service is in running state.
2. Perform a Verification Test as follows:
   a. Access the following URL in an **Incognito** or **Private Browsing** window: *https://localhost:8999/appviewx/rest/help*.
   b. Upon accessing the URL, a dialog box will appear requesting a certificate to be chosen.
   c. Please select the AppViewX issued client certificate from the Installer package or choose the required certificate if any custom certificate is used for authentication.

> **Note:** The same custom certificate has to be uploaded in the AppViewX CERT+ Application when configuring the Windows Gateway

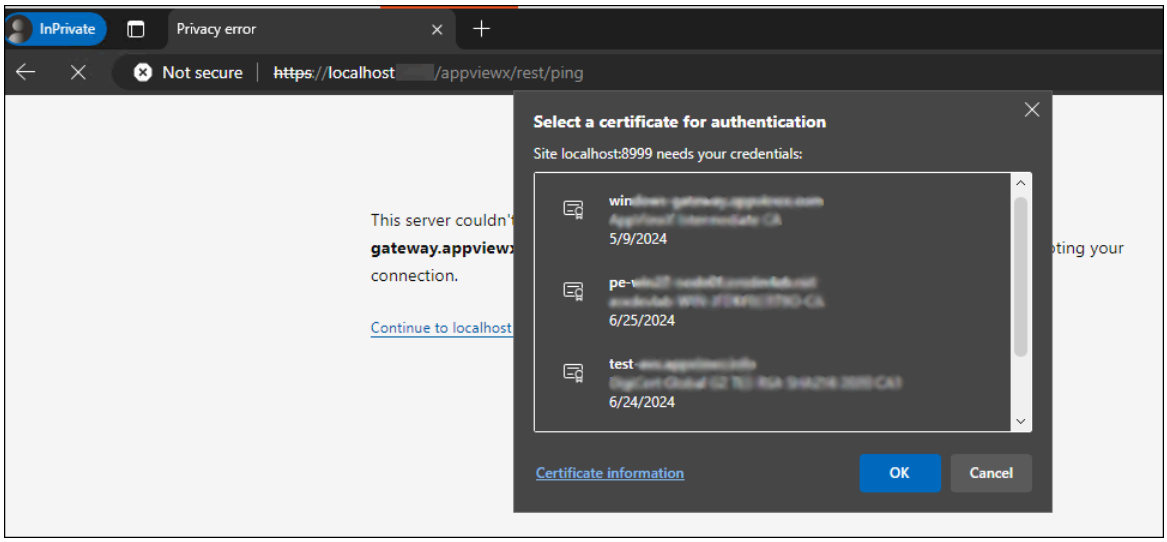
Sample output:



   d. The browser should then display the available services as a response.

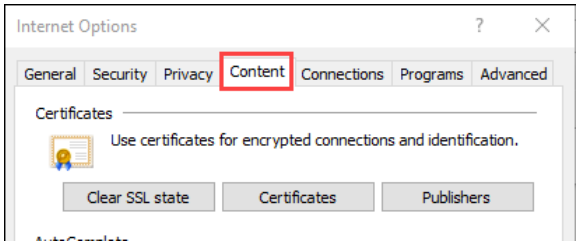
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Sample output



3. To verify the Windows AppViewX Gateway installation on Internet Explorer, import the client authentication certificate **ClientCertificateGateway.pfx**, from the download package (password: **appviewx**).

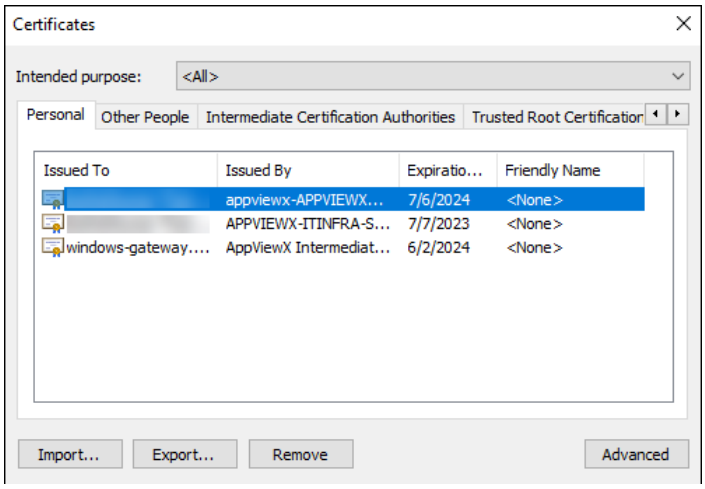
   a. Navigate to Internet Explorer's **Settings** > **Internet Options**, and then click the **Content** tab.



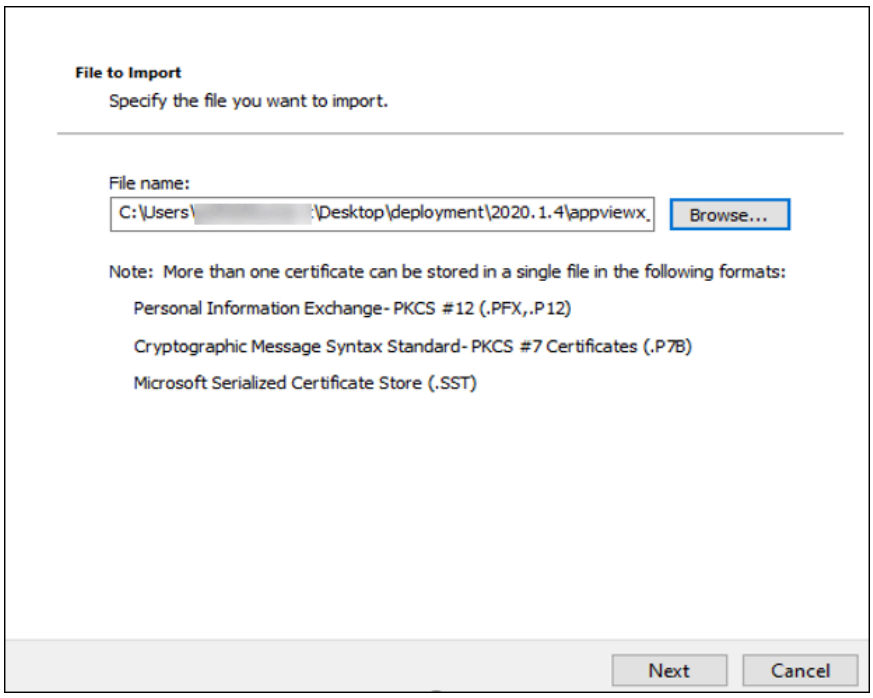
   b. Click the **Certificates** button.

   The **Certificates** popup window opens.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



c. Click the **Import** button on the **Certificates** page.



d. Go to the URL in the format: **https://hostname:portnumber/appviewx/rest/help**. For example: https://10.10.10.10:8999/appviewx/rest/help

The page displayed confirms the accessibility and installation of the service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operations at https://localhost:8999/appviewx/rest

This page describes the service operations at this endpoint.

Uri	Method	Description
BindCertificateToGateway	POST	Service at https://localhost:8999/appviewx/rest/BindCertificateToGateway
BindCertificateToSite	POST	Service at https://localhost:8999/appviewx/rest/BindCertificateToSite
BindSQLServerCertificate	POST	Service at https://localhost:8999/appviewx/rest/BindSQLServerCertificate
BootPropertiesReader	POST	Service at https://localhost:8999/appviewx/rest/BootPropertiesReader
CertDeviceInfo	POST	Service at https://localhost:8999/appviewx/rest/CertDeviceInfo
CheckConnection	POST	Service at https://localhost:8999/appviewx/rest/CheckConnection
CreateAndSubmitRequest	POST	Service at https://localhost:8999/appviewx/rest/CreateAndSubmitRequest
CreateCSR	POST	Service at https://localhost:8999/appviewx/rest/CreateCSR
CreateCSRKey	POST	Service at https://localhost:8999/appviewx/rest/CreateCSRKey
DeleteFile	POST	Service at https://localhost:8999/appviewx/rest/DeleteFile
DeleteKeys	POST	Service at https://localhost:8999/appviewx/rest/DeleteKeys
DeviceInfo	POST	Service at https://localhost:8999/appviewx/rest/DeviceInfo
DiscoverCertificates	POST	Service at https://localhost:8999/appviewx/rest/DiscoverCertificates
DiscoverCertStoreCertificates	POST	Service at https://localhost:8999/appviewx/rest/DiscoverCertStoreCertificates
DiscoverFileCertificates	POST	Service at https://localhost:8999/appviewx/rest/DiscoverFileCertificates
DiscoverIBM	POST	Service at https://localhost:8999/appviewx/rest/DiscoverIBM
DiscoverKeys	POST	Service at https://localhost:8999/appviewx/rest/DiscoverKeys
ExecuteScriptInPowershell	POST	Service at https://localhost:8999/appviewx/rest/ExecuteScriptInPowershell
ExecuteWLSTScript	POST	Service at https://localhost:8999/appviewx/rest/ExecuteWLSTScript
ExtractCertificate	POST	Service at https://localhost:8999/appviewx/rest/ExtractCertificate
GetCertStores	POST	Service at https://localhost:8999/appviewx/rest/GetCertStores
LatestLog	POST	Service at https://localhost:8999/appviewx/rest/LatestLog
MicrosoftCAs	POST	Service at https://localhost:8999/appviewx/rest/MicrosoftCAs
MqConnector	POST	Service at https://localhost:8999/appviewx/rest/MqConnector
Ping	GET	Service at https://localhost:8999/appviewx/rest/Ping
PushAndBindCertificate	POST	Service at https://localhost:8999/appviewx/rest/PushAndBindCertificate
PushCertificate	POST	Service at https://localhost:8999/appviewx/rest/PushCertificate
PushDiscoveredCertificates	POST	Service at https://localhost:8999/appviewx/rest/PushDiscoveredCertificates
ReadFile	POST	Service at https://localhost:8999/appviewx/rest/ReadFile
ReadMultipleFiles	POST	Service at https://localhost:8999/appviewx/rest/ReadMultipleFiles
RemoveCertificateFromStore	POST	Service at https://localhost:8999/appviewx/rest/RemoveCertificateFromStore
RemoveSiteBinding	POST	Service at https://localhost:8999/appviewx/rest/RemoveSiteBinding
RevokeCertificate	POST	Service at https://localhost:8999/appviewx/rest/RevokeCertificate
SaveKeys	POST	Service at https://localhost:8999/appviewx/rest/SaveKeys

Note: In the event that a custom client authentication certificate is used, ensure that the CRL mentioned in the certificate is reachable from the AppViewX Windows Gateway hosting server.

Note: The steps to import the client certificate will differ depending on the web browser.

e. To register the AppViewX Windows Gateway with AppViewX, navigate to the AppViewX Cert+ (on the SaaS deployment) admin UI/UX, and then **Settings** > **Certificate**.

Note: To add the AppViewX Windows Gateway for

- Microsoft Enterprise CA integration, see Microsoft Enterprise CA.
- Microsoft Standalone CA integration, see Microsoft Standalone CA
- Microsoft Device integrations, refer to the following sections:
  - Microsoft IIS
  - Microsoft PC
  - Microsoft Server
  - Microsoft SQL

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

f. Register the gateway using the following URL format: **https://hostname:portnumber/appviewx**. For example: https://10.10.10.10:8999/appviewx

Note:

- The AppViewX's custom client authentication uses CRL and OCSP as proposed by Microsoft. If you choose to use Microsoft's client authentication then comment the config file as below:

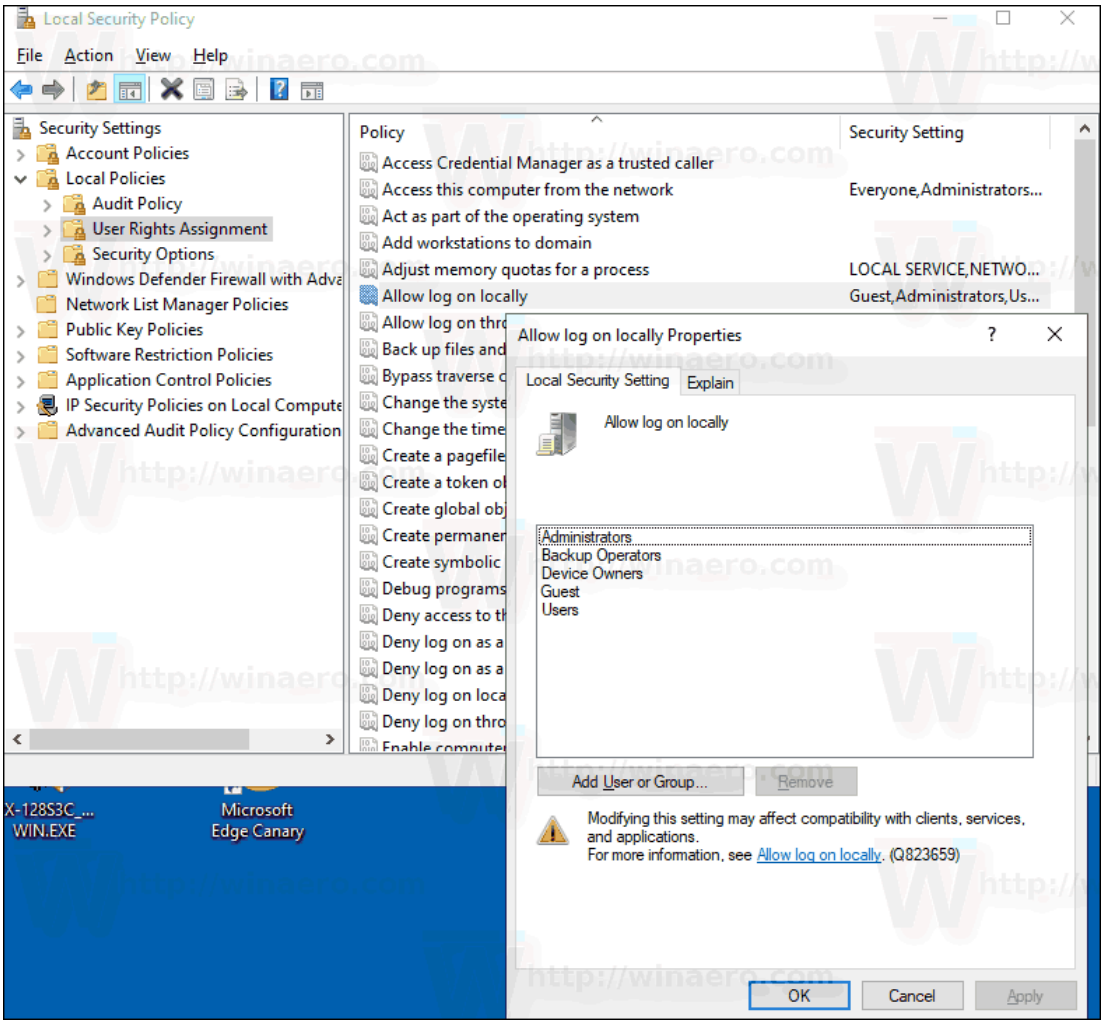
```
<!--<serviceCredentials>
<clientCertificate>
<authentication certificateValidationMode="Custom"
customCertificateValidatorType="AppViewX.CertPlus.Service.CustomValidator,  AppViewX.CertPlus.Service" />
</clientCertificate>
</serviceCredentials>-->
```

- AppViewX recommends customers not to change this default authentication configuration provided by AppViewX.
- Refer Appendix A for the prerequisites for managing the Windows Server infrastructure and Troubleshooting for troubleshooting the target machine.

Step 5: Managing a Target Server

To manage a target server with different credentials, the user account can be configured using the AppViewX user interface. Enable the **Allow log on locally** user rights assignment security policy for the account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Non-Admin Service Account

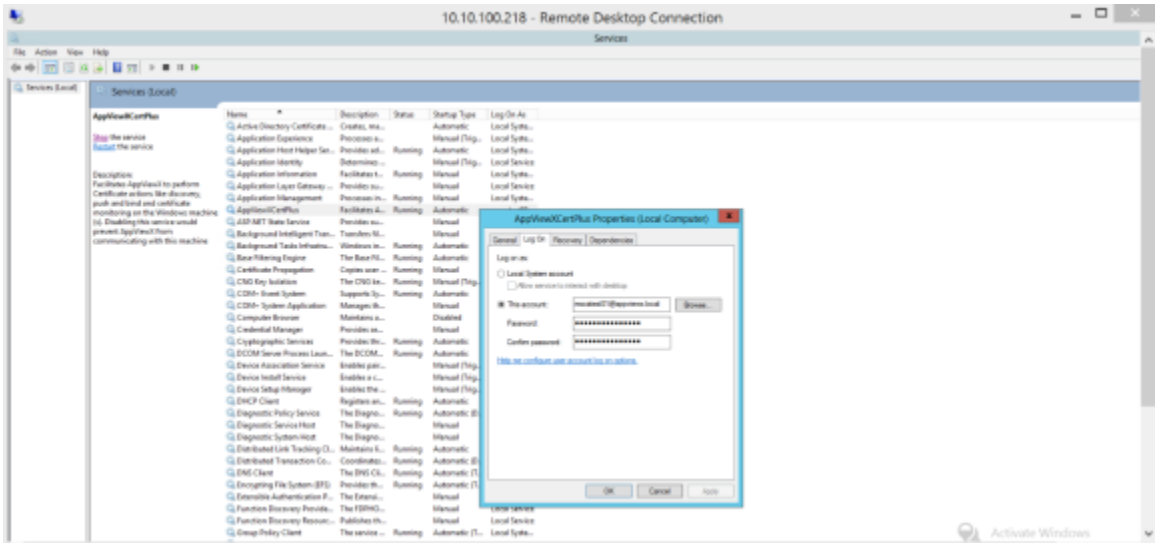
- The AppViewX Windows Gateway can be installed using a service account that is part of the local administrator group account.
- In this case, the following command has to be executed from the PowerShell:

```
netsh http add urlacl url=https://+:8999/appviewx/user=Username@domainname
```

- In the above command, the value for `user = <domainserviceaccount>` and the `URL` must be changed respectively.
- On the Regedit path, "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\AppViewXCertPlus" add the service account and give Full Control permission.
- On the Installation path of the application, the user needs permission to read and write.
- If the network has a policy that the service account cannot be part of the administrator group or that the service account is only a part of the user group, then:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The AppViewX Windows Gateway is installed using an admin account.
- It is then associated with the service account in **services.msc**, by adding the account in the properties of the AppViewXCertPlus service. Refer to the following image.



- Once this is done, stop and start the `AppViewXCertPlus Service` in `services.msc`.

Step 6: Disabling Current Operating System Information

On the https header, modify the registry.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters] "DisableServerHeader"=dword:00000002
```

Uninstalling the AppViewX Windows Gateway

Uninstalling AppViewX Windows Gateway involves the following steps:

1. Go to Windows control panel, select **Add or Remove program**.
2. Select **AppViewX.CertPlus.Installer**, and then click on **Uninstall** button.

Updating AppViewX Windows Gateway

Before updating the AppViewX Windows Gateway to a newer version, the old version of the AppViewX Windows Gateway should be uninstalled. Follow the instructions in Chapter 5 to uninstall AppViewX Windows Gateway.

After uninstalling the older version of AppViewX Windows Gateway, proceed with the installation of the new AppViewX Windows Gateway. Refer Chapter 2 for instructions on Installing the AppViewX Windows Gateway.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Appendix A

Appendix B

Onboarding Microsoft Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the ADC tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The Device details page is displayed.
4. Select **Microsoft Server** logo from the Vendors list. The following screen is displayed.
5. In the **Server Details** section button, enter details as mentioned below.

Server Details - Fields Description Table

Field Name	Description
Server Type	Select Server Type as **Microsoft Server**.
***Server name**	Enter the name of the designated Microsoft server.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Apache server.
Communication mode	Select the *Gateway* or *SSM* protocol to be used for communication between the AppViewX node and the Microsoft server. Gateway is the preferred communication mode.
Host name	Enter the hostname of the server to be onboarded. **Note:** If the Microsoft Server is configured for the **integrated** Windows Gateway mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Name	Description
Cert sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list. • Manual entry • Gateway credentials • Credential List - AppViewX AppViewX also supports the following external credential types: • HashiCorp • CyberArk • BeyondTrust • Thycotic If **Communication mode** = **SSM**, then **Credential list - cloudAccount** is supported.
***Username**	This field is displayed only if **Credential Type** = **Manual Entry**. Enter the username for authentication. **Note:** The username must be added with the domain in the following format: <username>@<domain>.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Name	Description
***Password**	This field is displayed only if **Credential Type** = **Manual Entry**. Enter the password for authentication.
***Credential List**	This field is displayed only if **Credential Type** = **Credential List - AppViewX**. Select the configured credentials value or Default from the dropdown list.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Field Name	Description
Credential Type	Select the type of credential from the dropdown list that will be entered in the username and password field. • Manual entry • Gateway credentials • Credential List - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example:* i-02573cafcftext

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field Name	Description
	Note: Click the (**Settings**) icon next to the field to configure the ARN Advanced Settings.
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2 **Note:** Click the (**Settings**) icon next to the field to configure the S3 Advanced Settings.
Proxy required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

7. Enter the **Windows gateway details**.

Note: This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Prerequisites for using the Integrated Windows Gateway mode **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Select gateway**	From the following options, select the gateway: • New • Existing
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway** and is non-editable.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
**: Mandatory fields*	

8. In the **Vendor Specific Details** section, select/enter the details as follows.
   If **Communication mode** = **Gateway** the fields are as follows:

Vendor Specific Details - Field Description Table

Fields	Description
***Services**	Select checkbox values as **MS Server**, or **Exchange Server**, or **Windows Gateway** or all. The default value is **MS Server**. **Note:** • Selecting all of the services will discover the certificates from MS Server, Exchange Server, and Windows Gateway. • If no services are selected, the service implementation will default to MSServer and CSR generation will be disabled. • The **Exchange Server** option is not supported for **Windows Gateway Mode** = **Integrated** and **SSM**. • Windows Gateway service can be used to enable the CLM support for the Windows GW certificate.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Vendor Specific Details - Field Description Table

Fields	Description
***Services**	For SSM the default services enabled is **MS Server**. (Exchange Server is not supported in the cloud).
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance Id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example*: i-02573cafcftext **Note:** Click the (**Settings**) icon next to the field to configure the ARN Advanced Settings.
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2 **Note:** Click the (**Settings**) icon next to the field to configure the S3 Advanced Settings.
Proxy Required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

9. In the **Certificate details** section, select/enter the details as follows.

Note: The **Certificate details** section will not be displayed if **Communication mode** = **Gateway** and **Services = Exchange Server** (in the Vendor specific details)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Details - Field Description Table

Fields	Description
***Keystore Credential Type**	Select the type of credential from the dropdown list. • Manual entry • Credential List - Thycotic **Note:** If **Credential list - Thycotic** is selected, the ***Keystore Credential Name** dropdown field is displayed. Select any of the preconfigured credential values.
Certificate location	Enter the directory/path where the application is installed. *Example*: C:\Microsoft\ADFS\
Certificate Password	Enter the certificate password. This field is only displayed for Keystore Credential Type = Manual entry)
**: Mandatory fields*	

10. Click **Add.**
    Once the server is added successfully, the path will be listed in the table.
11. *(optional step)* Click the (Delete) icon, if you want to delete the server path from the list.
12. Click **Save**
    The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Discovering Certificates for Microsoft Server

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding and Pushing Certificates to Microsoft Server

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Microsoft Server

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Microsoft Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ABAP server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, from the dropdown list, select one of the following options:
   - **MS Server**
   - **Exchange Server**
   - **Windows Gateway**

Note: If you have selected **Exchange Server**, profiles will be displayed in the format, **Server type : Service name : Node details**.

4. Under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For MS Server: Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select the location to which the certificate will be pushed: • **File System** (a storage location on your computer) • **Certificate Store** (a specialized location within the operating system for managing digital certificates)
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Credential Type**	This field is displayed for the JKS certificates. From the dropdown list, select the source of the access credentials.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	This field is displayed for the **PEM**, **DER**, and **PKCS#7** certificates. The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***KeyStore Password**	This field is displayed for JKS certificate types. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
Alias Name	This field is displayed for the PKCS#12 and CERTDB certificate types.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private key entry password	This field is displayed for the JKS certificates. Enter the password required to decrypt the private key associated with the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate Certificate Alias Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. This field is not displayed for the JKS certificate types. Enter the alias name of the intermediate certificate file.
***Root Certificate Alias Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the alias name of the root certificate file.

For Exchange Server: Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	The certificate type is defaulted to the following values • For AppViewX CSR generation - certificates which have private key, **PKCS#12(*.p12)** is the supported certificate format. • For Endpoint CSR generation **PKCS#7(*.p7b)** is the supported certificate format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The password field in not set for **PKCS#12(*.p12)** since its a transactional password and handled by AppViewX.
***Friendly Name**	• For **PKCS#12(*.p12)** it is the user specified input. • For **PKCS#7(*.p7b)** certificate type, the friendly name is the common name of the certificate specified at the time of Endpoint CSR generation. During the push operation the common name is populated in the friendly name field (it is not editable).
Services	From the dropdown list, select one from the following services: • **POP** • **IIS** • **SMTP** • **IMAP**
Restart Service	This field is displayed only when **Services** = **IIS**. To restart the IIS service after the certificate is pushed, to ensure all changes have taken effect as required, select this checkbox.

For Windows Gateway: Field descriptions for the Certificate Details

Field	Description
Location Type	The **Certificate Store** option is selected by default—a specialized location within the operating system for managing digital certificates. (**File system** is disabled).
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. **Note:** Root and intermediate names cannot be entered for this CSR/Certificate. If auto-push is enabled for CSR, try again after the certificate is generated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings

This is applicable for all service/devices such as Microsoft Server, Microsoft Exchange Server, Windows Gateway.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

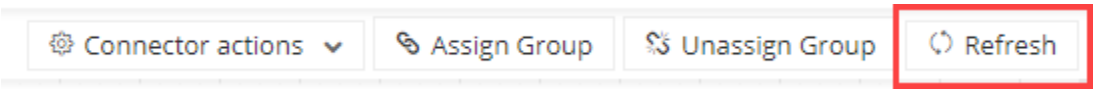
The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

> **Note:** While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.
   The holistic view of the selected certificate is displayed.

   > **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
    a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
    The **Group** page is displayed.
    b. From the **Name** field, select the required certificate group.
    The **Group : Modify : <group name>** page is displayed.
    c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
    d. Click **Update**.
2. To enable auto push for the certificate connector:
    a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
    To add an application connector, follow the instructions given here.
    b. From the menu displayed, click **Edit**.
    The **Edit Application Connector** pop-up is displayed.
    c. Select the **Push automatically** checkbox.

    > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

    d. Click **Save**.
    The holistic view of the selected certificate is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

What's Next?

- Set alerts to be notified of all events and status changes in the certificate lifecycle.

Automating CLM for Microsoft IIS

The Microsoft IIS (Internet Information Services) server is a web server developed by Microsoft. It is used to host and serve web applications and websites on Windows Server operating systems. In a typical deployment, an IIS server device is configured with SSL/TLS certificates to secure communications and establish trust between the server and its clients.

Prerequisites

- Both the Windows gateway agent and the windows machine running Microsoft IIS must have administrative privileges.
- Ensure that PowerShell and WinRM tools are installed and running on the Windows machine.
- Verify that Microsoft IIS services are active on the Windows machine.
- At least one website must be configured on the Microsoft IIS server.
- If the Gateway type is selected as WMI, ensure that WMI is properly configured (optional).
- The user must have **read and write permissions** for the folder specified as the **discovery path** and the **push location**.
- The user must have the right **access permissions** to the drive, and the drive must be **configured in sharing mode** to allow discovery and push operations.
- To discover and push the certificate to the store, user should have **Read and write access to the trust store** (to discover and push certificates).

Limitations

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Certificates enrolled at the endpoint cannot be pushed to the file system, as this functionality is not supported in the application.
- External vault integration in Folder credential is not supported when the shared path credential differs from the onboarded device credential.

Onboarding Microsoft IIS

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft IIS** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft IIS server.
***Hostname**	Enter the hostname of the Microsoft IIS server that is to be onboarded. **Note:** If the Microsoft IIS server is configured for the integrated Windows Gateway mode, ensure that the hostname used is resolvable in the cloud connector. The usage of FQDN is preferred.
Data center	Choose the desired data center. It holds all the SSL What can you do next? that is to be retrieved from the Microsoft IIS server.
Cert Sync	Choose from any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	• *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft server device.

Credentials - Field Description Table

Fields	Description

***Credential Type**	Select the credential type from the dropdown.
	• *Manual entry* (default)
	• *Credential List - Appviewx*
	• *Gateway credential*
	• All supported external vaults
	
	Note:
	• If **Credential list - Appviewx** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
	• If **Gateway credential** is selected no other fields are displayed.
	• AppViewX supports the following external credential types:
	  • HashiCorp
	  • CyberArk
	  • BeyondTrust
	  • Thycotic

Certificate Location Details	By default, only the **Certificate store** option is selected for certificate discovery. If the user wants to discover certificates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	from the **Centralized file system**, they must select the corresponding checkbox, specify the certificate location. The certificate location supports both a shared path and a local file system directory; however, only one of these can be configured at a time. From the given location `pfx and p12 certificates will be discovered.` Choose a pre-configured password vault from the dropdown menu to parse the password protected certificates.
***Username**	Enter the designated username for authentication.. (field displayed for manual entry only)
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

7. Enter/Select the **Windows gateway details**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (enabled only in the SaaS and Managed Kubernetes installations).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Prerequisites for using the Integrated Windows Gateway mode **Note:** The integrated gateway functionality is not compatible with the following feature: • Server addition using the **import** feature
***Gateway type**	From the following options, select the required gateway type: • PowerShell • WMI **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • Remote • LocalSystem **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***FQDN**	**Note:** This field is displayed when **Gateway location** = **LocalSystem**. Enter the FQDN of the local system on which the Windows Gateway Agent will be installed.
***Port**	**Note:** This field is displayed when **Gateway location** = **LocalSystem**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Enter the port number of the local system on which the Windows Gateway Agent will be installed.
***Select gateway**	**Note:** This field is not displayed when **Windows Gateway Mode** = **Integrated**. From the following options, select the gateway: • New • Existing
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

Microsoft IIS Discovery

The discovery process for Microsoft IIS can leverage multiple sources, as outlined below:

- **File System Discovery**: Requires at least one file path to be specified during device addition.
- **Microsoft Certificate Store Discovery**: Automatically scans the server's certificate store for available certificates.
- **Shared Network Path Discovery:**IIS supports discovery through shared network paths. This means that within the network of the managed IIS device, the logged-in user can be granted access to a shared folder on another system. By specifying that shared network path in the certificate location, the discovery process can be performed successfully.

The **AppConnector** is created dynamically based on the discovery method used.

Connector Behavior for IIS

For certificates discovered from the File System in Microsoft IIS, both Push-only/Default connectors and detailed profile connectors are created. The available profiles depend on the selected push certificate type in the application connector.

Push Certificate Type Options

When adding or updating certificates in Microsoft IIS using the app connector, users can select the desired Push Certificate Type:

a. **Push Certificate:** You can only push certificates to the Certificate store or Centralized File System.
   - Only the Device Name profile is displayed for selection.
   - Profile naming convention:

     `{device_name}`

b. **Push and Bind Certificate:** You can push a certificate to the Certificate store and bind it to the IIS site.

   All detailed profile connectors are displayed for selection, using the convention described below:

   `MS IIS::<siteName>::<host/IP>:<port>:<hostname (optional)>:CS[:(SNI or protocol)]`

   - `<siteName>`: IIS site name or wildcard (*)
   - `<host/IP>`: Hostname or IP address, or *
   - `<port>`: Port number (e.g., 80, 443)
   - `<hostname (optional)>`: FQDN or specific hostname, if applicable
   - `CS`: Certificate Store indicator
   - `:(SNI or protocol)`: *(SNI)* if SNI enabled, *(http)* for HTTP profile, as applicable

   Examples:

   - `MS IIS::test:*:8090:CS`
   - `MS IIS::test:*:443:CS`

Copyright © 2025 AppViewX Inc. All Rights Reserved.

8. In the **Certificate location details** section, enter the details as indicated below.

Certificate Location Details - Field Description Table

Fields	Description
***Location type**	Select to the checkbox for *Certificate store* or *Centralized file system* or both as the location type.
***Certificate location**	Enter the directory or path where the certificate is stored. *Example*: C:\Cert\folder
***Password vault**	Select any of the preconfigured password vault values. None is selected by default.
**: Mandatory fields*	

9. In the **Folder credential details** section, enter the details as indicated below.

Folder Credential Details - Field Description Table

Fields	Description
***Folder credentials**	Select from • Use gateway credential • New • Use device credential (disabled by default)
***Credential type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List - Appviewx* • *Credential List - CyberArk* • *Credential List - Thycotic* • *Credential List - Hashicorp* • *Credential List - BeyondTrust* **Note:** If **Credential list - Appviewx** or **Credential list - CyberArk** is selected, the ***Credentials list** dropdown field is displayed. Select any of the preconfigured credential values.
***Username**	Enter the designated username for authentication. (field displayed for manual entry only)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Password**	Enter the secure password. (field displayed for manual entry only)
**: Mandatory fields*	

10. Click **Save**.
    The Microsoft IIS device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Discovering Certificates for Microsoft IIS

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding and Pushing Certificates to Microsoft IIS Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Microsoft IIS

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **IIS**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.
***Push Certificate Type**	Select from the following options: • **Push Certificate** You can only push certificates to the Certificate store or Centralized File System. • **Push and Bind Certificate** You can push a certificate to the Certificate store and bind it to the IIS site.

Based on the information entered here, the **Server selection** section is populated with the list of available IIS devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select where the certificate to be pushed is located: • **Certificate Store**: A repository that stores certificates and their associated keys • **Centralized file system**: A file server that stores certificate files

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Store	This option is displayed only when **Location Type** = **Certificate Store**. Within the certificate store, select the location where the certificates are stored from the following options: • **Personal store**: A location where user-specific certificates, such as those used for encryption and authentication, are stored • **Web hosting store**: A location where certificates used for web server configurations are stored
***Friendly name**	Enter the certificate friendly name assigned in the CSR generated for requesting/ enrolling the certificate
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
***Bind type**	**Note:** This field is displayed when the **Push Certificate Type** is selected as **Push and Bind Certificate**. To manage the SSL/TLS certificates for websites, select a bind type from the following options: • **Update Certificate Only**: Update the SSL/TLS certificate used by an existing site binding on the web server. It replaces the current certificate with a new one without modifying any other settings associated with the site binding (such as the hostname or port). • Update Site Binding: Update the SSL/TLS settings for an existing site binding on the web server. It allows you to update not only the certificate but also other settings associated with the site binding, such as the hostname, port, and SSL/TLS protocol settings. • **Create New Site Binding**: Create a new site binding on the web server for the specified hostname, port, and IP address (if applicable) and associates it with the specified SSL/TLS certificate. This is typically used when you want to add a new website or domain to the web server and configure SSL/TLS settings for it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- **Certificate Store Push**
  - If the certificate is created **at the endpoint** (private key on the device):
    - The **server certificate** is pushed in **.pem** format.
    - The **root and intermediate certificates** are pushed in **.pfx** format.
  - If the certificate is created **in AppViewX** (private key within AppViewX):
    - The **server**, **root**, and **intermediate certificates** are all pushed in **.pfx** format.
- **File System Push**
  - Only a **single .pfx file** (containing the certificate, private key, and root/intermediate certificates if available) is pushed to the specified file system location.
- **Supported Certificate type for File System Push**
  - PKCS#12 (.pfx)
- When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:
  - **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
  - **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings
- File system push is supported only when the Centralized File System option is enabled on the onboarding page.
  - The Certificate Location field is optional. By default, the certificate will be pushed to the directory specified during onboarding.
  - The password for the certificate pushed to the file system is retrieved from the vault configured during onboarding.

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system. **Note:** Overwrite option is disabled by default for Microsoft IIS.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

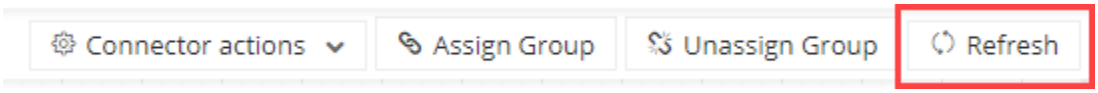
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

> **Note:** While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.

The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Automating CLM for Firewall

Onboarding a Firewall Device

Adding a CheckPoint Device

Refer to Automating CLM for CheckPoint

Adding a Cisco Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port numbers 22 (SSH)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Certificates are fetched by issuing a direct command to the device through SSH.

Note: For Visual Workflow action items, you will require credentials with write privilege.

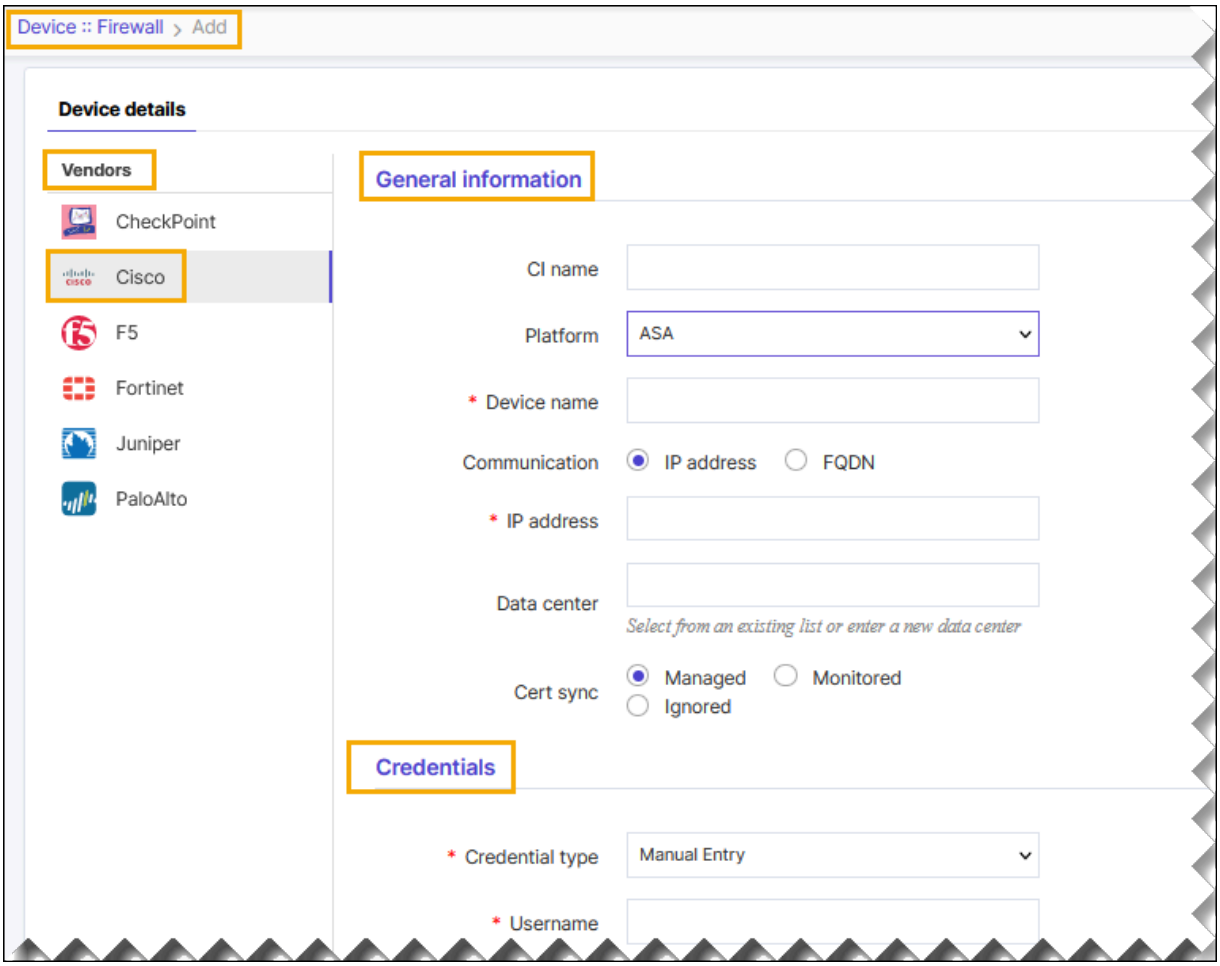
Configuring a Cisco Firewall Device

Prerequisites

To add a Cisco device:

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **Cisco** vendor from the left side bar

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the dropdown list. The available option is ASA.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

5. Enter the field information in the **Credentials** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the dropdown list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the privilege password.
**: Mandatory fields*	

6. Enter the field information in the **Secondary device information** section as follows:
   - **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
   - **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
   - **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

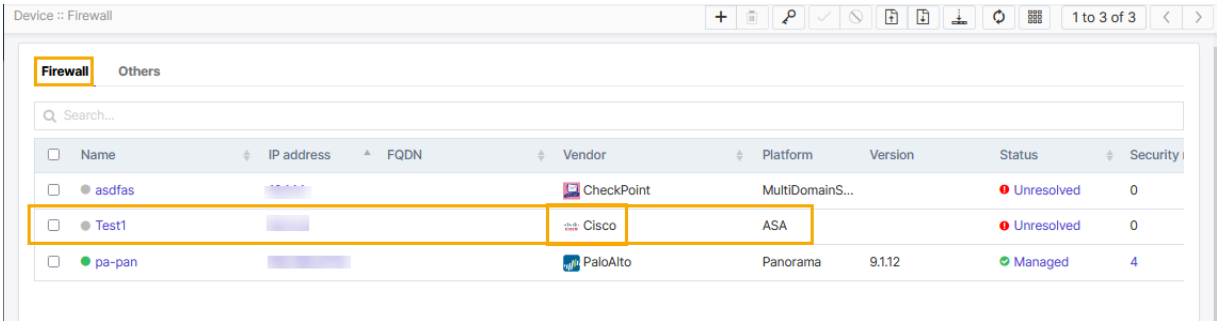
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the Cisco Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Adding a F5 Firewall Device

Configuring a F5 Firewall Device

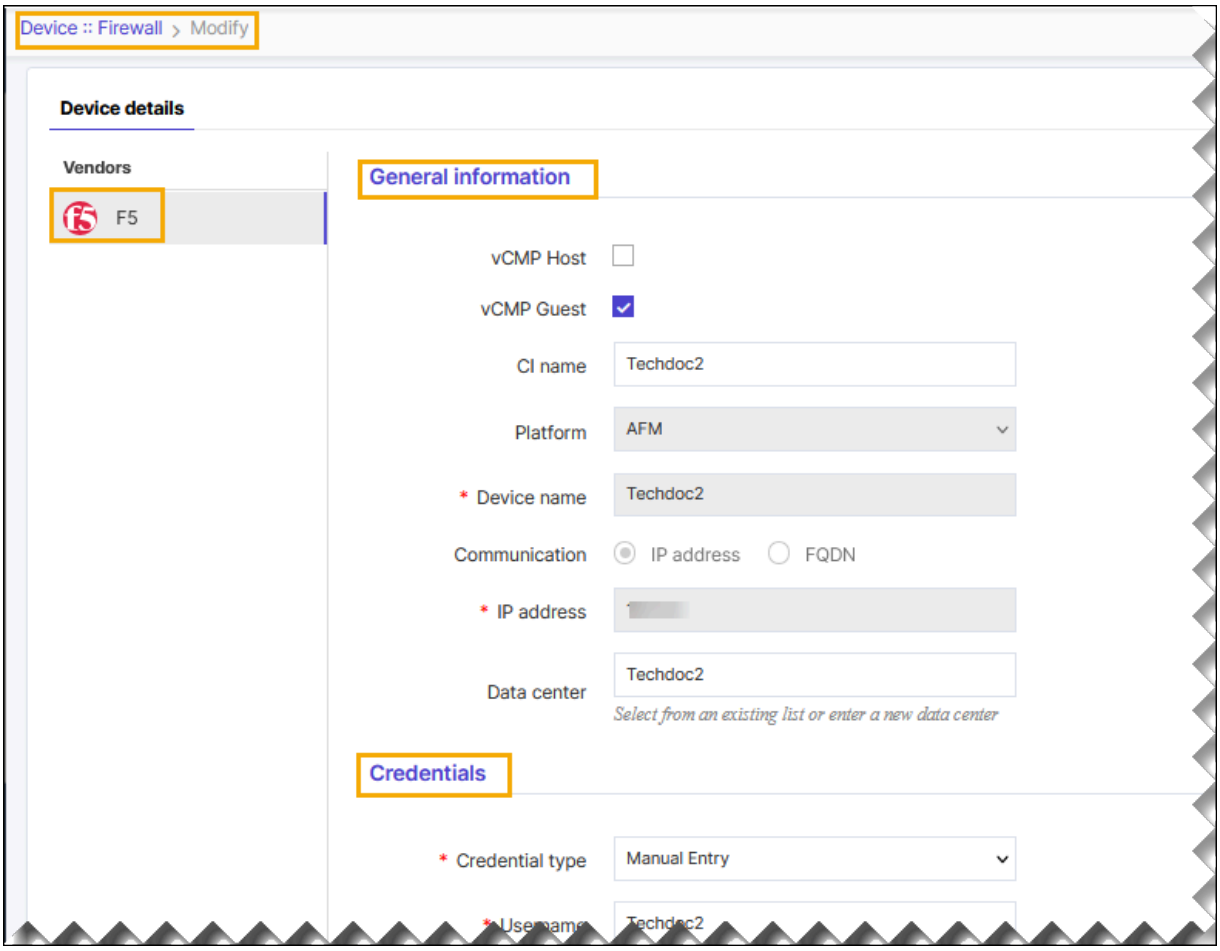
To add a F5 device:

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Add** page appears.

3. Select the **F5** vendor from the left side bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
vCMP Host	Select the check box to add host based device if required.
vCMP Guest	Select the check box to add device as guest if required..
CI name	Name of the CI.
Platform	Select the platform from the dropdown list. The available option is AFM.
***Device name**	Unique custom identifier of your device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

5. Enter or select the field information in the **Credentials** section:

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the privilege password.
**: Mandatory fields*	

6. **Note:** This step is applicable only if you have selected **vCMP Host** check box in the **General Information** section.

   Enter or select the field information in the **Secondary device information** section as follows:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
- **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
- **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

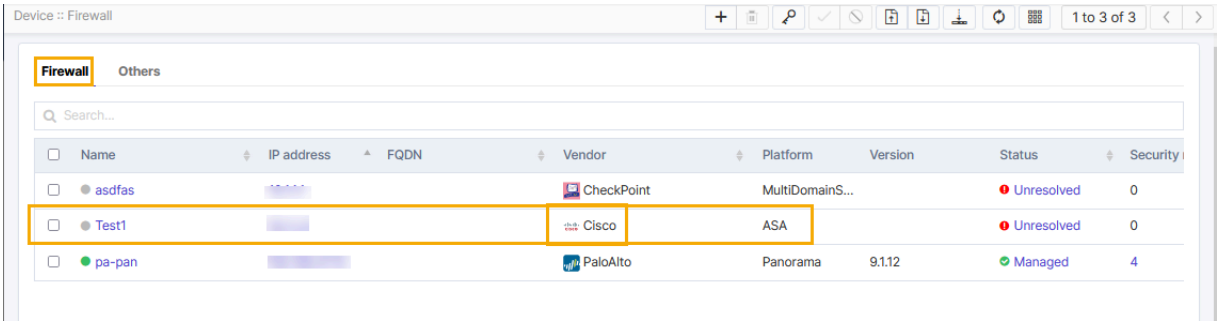
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the F5 Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Adding a Fortinet Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**: Username/Password
- **Services and Port for AppViewX Communication**: Port number 22 (SSH)

> **Note:** For Visual Workflow action items, you will require credentials with write privilege.

Configuring Fortinet Firewall Device

To add a Fortinet device:

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **Fortinet** vendor from the left side bar.
4. Enter the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select from the following options: • Fortigate • FortiManager
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the dropdown list or enter a data center name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
***SSH Port**	By default, it is 22.
**: Mandatory fields*	

5. Enter the field information in the **Credentials** section:

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. • If external credential types such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault are configured, then this credential type will be listed in the device addition screen. Choose the appropriate Credential Type from the dropdown list. If authentication relies on an external credential, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Api token	Enter the API token.
**: Mandatory fields*	

6. Enter the field information in the **Certificate specific details** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
Discover Private Keys	Select the check box.
Private Key Default Password	Enter the default password.

7. Enter the field information in the **Secondary device information** section as follows:
   - **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
   - **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
   - **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

   Note:
   - By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
   - By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

8. Click the **Save** button to add an Firewall device.

   Note:
   - To discard the changes, click the Cancel button.

   A pop-up message is displayed as **Device added successfully**.

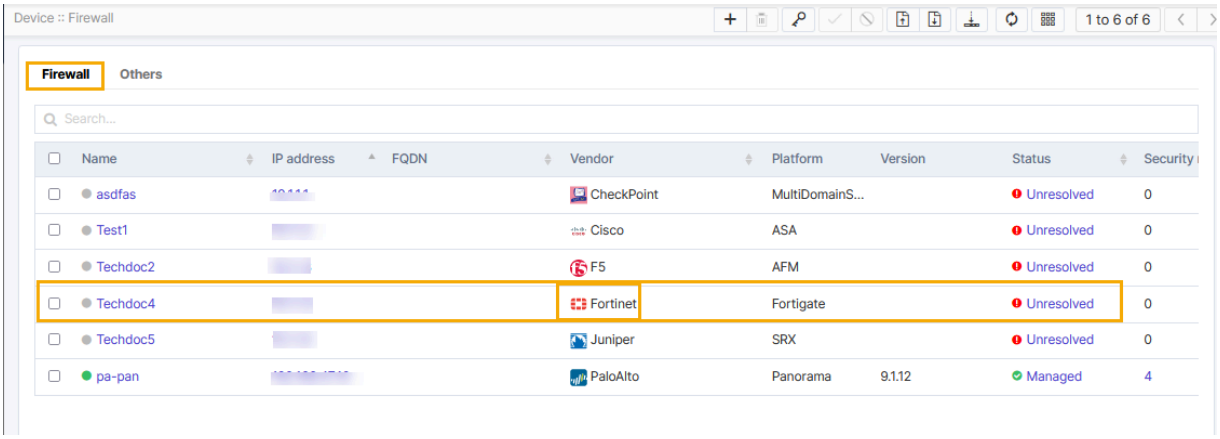
Validating the Device

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Search the device name and validate whether the device is added successfully.



CLI Commands

Minimum required permissions

- **Version of device:** 6.x or above
- **License type:** Cert+ Only 16
- **Device management**

  Network > Configuration > Read Only (Communication and version check)

- **Certificate discovery**
  - System > Configuration > Read/Write (System Local Certificates, System Setting)
  - VPN > Read (VPN Profiles)
  - Firewall > Others > Read (SSL/SSH Inspection Profile)
  - User & Device > Read (User Authentication Setting Profile)
- **Certificate Push and Bind**
  - System > Configuration > Read/Write (Push to System Local Certificates, Bind System Server Certificate)
  - VPN > Read/Write (Bind to VPN Setting Profile, VPN Ipsec profile)
  - Firewall > Others > Read/Write (Bind to SSL/SSH Inspection Profile)
  - User & Device > Read/Write (Bind to User Authentication Setting Profile)

Operation	Command	Description
System Status	`get system status`	Displays system information such as firmware version, VDOM status, and system mode.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description
Configure VDOM	`config vdom`	Enters VDOM configuration mode to manage Virtual Domains.
Edit configurations	`edit ?`	Enters edit mode for a specific configuration object (e.g., VDOM, interface, etc.).
End	`end`	Ends the current configuration mode and applies changes.
Switch to global	`config global`	Switches to the global configuration context.
Configure System's console	`config system console`	Used to configure console settings; often used with set output standard for terminal output.
Set output to standard	`set output standard`	Sets the console output format to standard (non-JSON or non-table).
Show full CA certs (VPN)	`show full-configuration vpn certificate ca`	Displays full configuration of CA certificates used in VPN.
Show full CA certs	`show full-configuration certificate ca`	Displays full configuration of CA certificates in the system.
Show full local certs (VPN)	`show full-configuration vpn certificate local`	Displays full configuration of local VPN certificates.
Show full local certs	`show full-configuration certificate local`	Displays full configuration of local certificates in the system.
Show IPSec VPN config	`show vpn ipsec {CONFIGURATIONS}`	Displays IPsec VPN configurations.
Show SSL VPN settings	`show vpn ssl settings`	Displays current SSL VPN settings.
Show user settings	`show user setting`	Displays user authentication settings.
Show SSL/SSH profiles	`show firewall ssl-ssh-profile`	Displays SSL/SSH inspection profiles used in firewall policies.
List CA cert names (VPN)	`show full-configuration vpn certificate ca ?`	Lists available CA certificate names in VPN configuration.
List CA cert names	`show full-configuration certificate ca ?`	Lists available CA certificate names in the system configuration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description
List local cert names (VPN)	`show full-configuration vpn certificate local ?`	Lists available local certificate names for VPN.
List local cert names	`show full-configuration certificate local ?`	Lists available local certificate names configured on the device (non-VPN).
Set CA certificate	`set ca \"{CERT_CONETNT}\"`	Sets the CA certificate content during certificate configuration.
Set private key	`set private-key \"{PVT_KEY_CONETNT}\"`	Sets the private key content for a certificate.
Set certificate content	`set certificate \"{CERT_CONETNT}\"`	Sets the actual certificate content.
Set password	`set password`	Sets a password (often used when importing password-protected keys/certs).
Unset password	`unset password`	Removes a previously set password from the configuration.
Configure SSL VPN settings	`config vpn ssl settings`	Enters configuration mode for SSL VPN settings.
Unset SSL VPN cert	`unset servercert`	Removes the currently configured SSL VPN server certificate.
Set SSL VPN cert	`set servercert {CERT_NAME}`	Sets the server certificate for SSL VPN.
Configure SSL/ SSH profile	`config firewall ssl-ssh-profile`	Enters configuration mode for SSL/SSH inspection profiles.
Unset SSL/SSH cert	`unset server-cert`	Removes the configured certificate from the SSL/SSH profile.
Set SSL/SSH cert	`set server-cert {CERT_NAME}`	Sets the server certificate for SSL/SSH inspection.
Configure global settings	`config system global`	Enters system-wide global configuration mode.
Set admin portal cert	`set admin-server-cert {CERT_NAME}`	Sets the certificate used for the FortiGate admin GUI (HTTPS portal).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Operation	Command	Description
Configure user settings	`config user setting`	Enters configuration mode for user authentication settings.
Set user auth cert	`set auth-cert {CERT_NAME}`	Sets the certificate used for user authentication.
Configure IPsec VPN	`config vpn ipsec`	Enters IPsec VPN configuration mode.
Append cert to IPsec VPN	`append certificate {CERT_NAME}`	Appends a certificate to the IPsec VPN configuration.
Generate certificate	`execute vpn certificate local generate`	Generate a local certificate on the device.

Pushing Server Certificates to the Device

The certificate can be pushed to the device in only PEM format.

Note: Starting from FortiOS version 5.4 and above, when pushing a certificate to FortiGate, if a certificate with the intended name is already present, a timestamp is automatically appended to the certificate name. This ensures the new certificate is successfully imported without conflict, while retaining the original.

Warning:

Fortigate does not allow importing a certificate that has already been imported earlier—even if you attempt to import it again under a different name or context. FortiOS maintains a checksum or fingerprint of certificates.

If a certificate with the same cryptographic material already exists in the system (for example, with the same subject, serial number, and public key), it will reject duplicates to prevent redundancy or configuration conflicts.

Profiles will be discovered irrespective of the cert sync option selected during device addition or during an on-demand discovery. The following profiles will be discovered currently in AppViewX:

- **Shared location:** Denotes a push-only operation which pushes a certificate to the end device.

  Profile convention : {DeviceName}::System/Vdom name

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **SSL VPN Settings:** SSL VPN allows remote users to securely connect to the corporate network using an encrypted SSL tunnel via a web portal or FortiClient. Apushed certificate can be associated to SSL-VPN setting if it is enabled.

  Profile convention : {DeviceName}::System/Vdom name::SSL VPN Setting:SSL VPN Setting

- **SSL/SSH Inspection Profile:** SSL/SSH inspection profiles inspect encrypted traffic (HTTPS/SSH) for threats or policy enforcement. Apushed certificate can be associated to any inspection profile if it is configured with Protecting SSL Server option.

  Profile convention : {DeviceName}::System/Vdom name::SSL/SSH Inspection Profile:{Inspection profile name}

- **System Setting Https Server Certificate:** This controls which certificate is used to secure access to the Fortigate administrative web interface. Apushed certificate can be associated to the System administration setting server certificate.

  Profile convention : {DeviceName}::System::System Setting Https Server Certificate

- **User Authentication settings:** Defines how users authenticate to Fortigate (e.g., captive portal, VPN, web portal). Ensures only clients with valid certificates can authenticate, enhancing security. Apushed certificate can be associated to the User authentication setting server certificate.

  Profile convention : {DeviceName}::System:User Authentication settings:User Authentication settings

- **IPSec VPN Profile:** IPSec VPN allows site-to-site or remote client VPN connections using the IPSec protocol suite. Apushed certificate can be associated to the IpSec tunnel configured in the device.

  Profile convention : {DeviceName}::System:IPSec VPN Profile:{TUNNEL_NAME}

Backing Up Certificates

Before a bind operation, a backup will be taken for the currently associated certificate so that a rollback can be performed once the new certificate is associated.

Binding Certificates

Certificates can be bound for profile connectors. These connectors include all the connectors other than the shared location connector.

The selected selected certificate will be pushed to the shared location first and then the certificate will be associated to the selected profile.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Rolling Back Certificates

In the event of a rollback, the system restores the previous state by unbinding the current certificate, pushing and binding the backed-up certificates to the selected profile.

CSR Generation

Note: Generation of CSR can be performed for a Fortigate device during certificate enrollment. The Partition name, CSR File Name, and Key File Name have to be provided.

Adding a Juniper Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port number 22 (SSH)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Not supported

Note: For Visual Workflow action items, you will require credentials with write privilege.

Configuring a Juniper Firewall Device

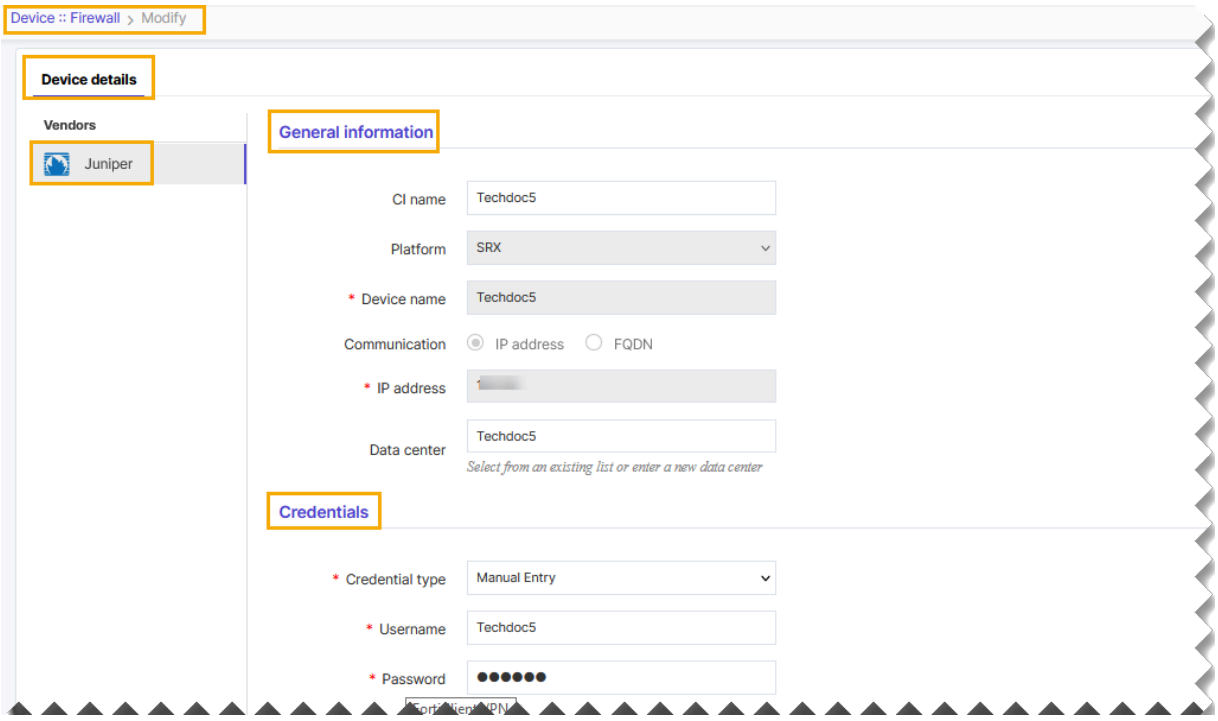
To add a Juniper device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Add** page appears.

3. Select the **Juniper** vendor from the left side bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • SRX.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

5. Enter or select the field information in the **Credentials** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the password.
**: Mandatory fields*	

6. Enter or select the field information in the **Secondary device information** section as follows:

   • **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.

   • **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.

   • **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

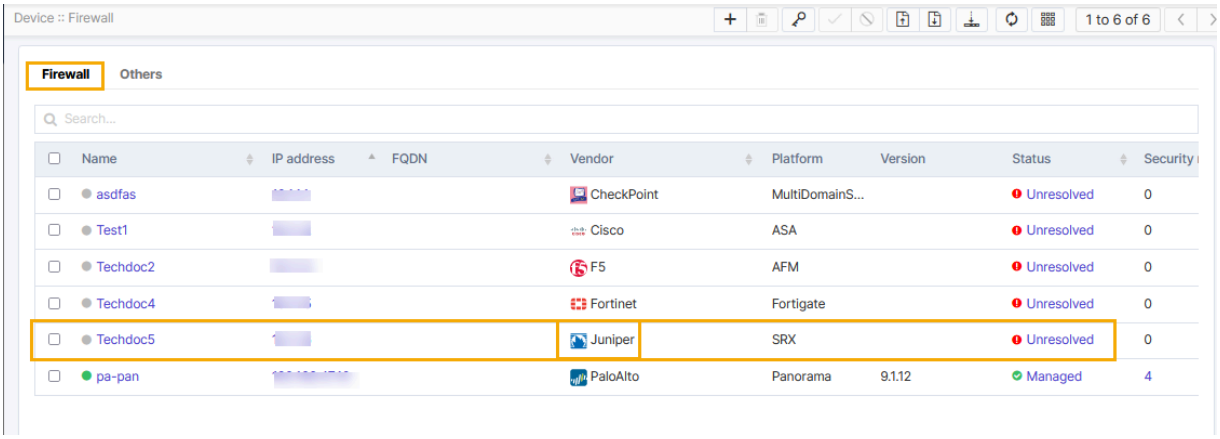
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the Juniper Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Adding a Palo Alto Firewall Device

Refer to Automating CLM for Palo Alto.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Discovering Certificates for Firewall

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

   Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Note: Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Firewalls**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Devices window	A list of all the managed firewall devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding and Pushing Certificates to Firewall Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding Application Connectors for Firewalls

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Firewall**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select the required firewall vendor. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **Profile Selection** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

2. To select the device(s) to which the certificate will be pushed, under **Profile Selection**:

   a. For **CheckPoint** Vendor, to filter the available profiles, from the dropdown menu for Available profiles, select a value from the following options:
   - **Admin Portal**
   - **HTTPS Inspection**.

   b. For **PaloAlto** vendor, to filter the available profiles, from the dropdown menu for Available profiles, select a value from the following options:
   - **PaloAlto Firewall**
     - Shared location
     - SSL/TLS Service profile
     - IKE Gateways
     - SSL Inbound Inspection Profiles
     - Authentication Profiles.
   - **Panorama**
     - Shared location
     - SSL/TLS Service profile
     - IKE Gateways
     - SSL Inbound Inspection Profiles
     - Authentication Profiles.

   c. From the list of **Available Devices** displayed, to select the target device(s) for pushing the certificate, click .

   The **Selected devices** list is updated automatically.

3. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Trust Point Name**	A trustpoint configuration is an element that includes details related to a certificate such as the certificate file, the private key file, the CA certificate, and other settings related to the certificate. In the **Trustpoint Name** field, enter the name of the trustpoint configured on the target system to which the certificate will be pushed.
Alias Name	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Password	Enter the password required to access the certificate file/trust store.
Private Key Passphrase	Enter the password required to access the private key file associated with the certificate.
Push to Firewall	To push the certificate when it is updated directly to the firewall, select this checkbox.
Trust Type	**Important:** Trust type is applicable only for server certificates issued by private CAs with a customized template that issues certificate to the PaloAlto device with **Key Usage** as **Certificate Signing** for certificates that have a private key. **Trust Type** defines how a firewall handles SSL/TLS traffic based on whether a certificate is trusted or untrusted. Select a trust type status from the following values: • **Forward Trust** Select this option to establish the firewall as a trusted third party (proxy) to the session between the client and the server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	For **Trust Type** = **Forward Trust**, if the server's certificate is valid (trusted) and signed by a known, trusted CA (like VeriSign, DigiCert, etc.), the firewall decrypts the traffic, inspects it, and then re-encrypts it using its own certificate, which is trusted by the client due to the configured CA. • **Forward Untrust** Select this option for the firewall to notify to clients when the server certificate is signed by a CA that the firewall does not trust. For **Trust Type** = **Forward Untrust**, if the server's certificate is self-signed or from an unknown CA, the firewall may re-encrypt the traffic using an untrusted certificate, causing the client to see a warning that the connection is not secure. **Note:** If the certificate trust type was already specified when configuring the certificate on the device, then upon discovery in AppViewX, the trust type field will reflect the same value as configured in the device port.

4. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

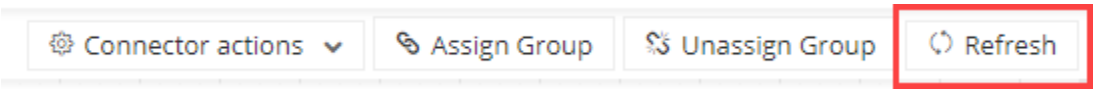
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Note: Every time a certificate is pushed to a shared location in Palo Alto Firewall / Panorama,the user currently needs to log into the device and manually commit the changes. Moving forward, pushing a certificate to the shared location will automatically trigger the commit process.
The push operation will only be marked as successful in AppViewX after the commit process successfully completes on the device.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.
   The holistic view of the selected certificate is displayed.

   > **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Automating CLM for Palo Alto

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

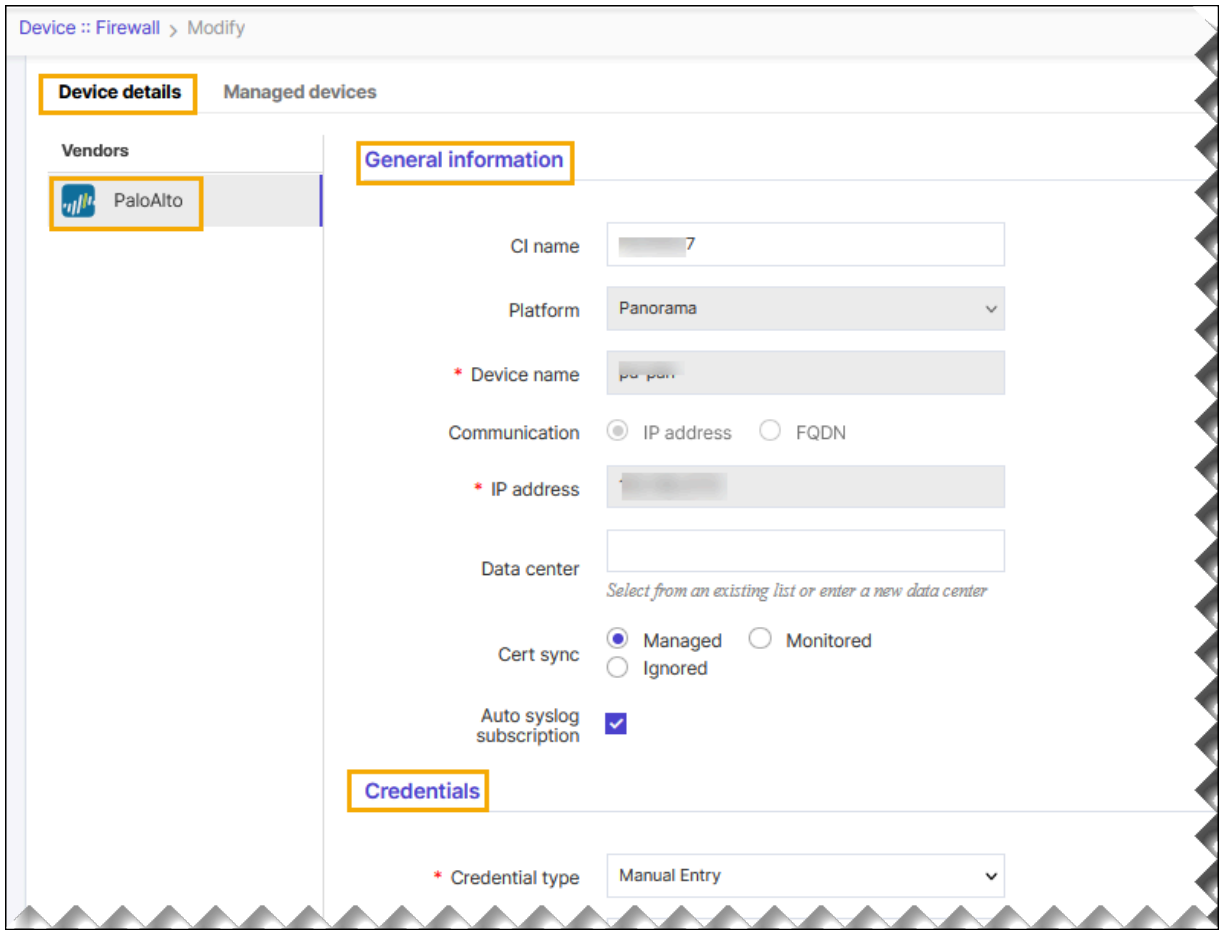
- **General prerequisites**:
  - Palo Alto Networks user assigned an Admin Role Profile with Configuration, Operational Requests, Commit, Export and Import privileges for the XML API.
  - Ensure communication between AppViewX and the firewall is enabled.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX
  - If authentication relies on an external credential such as Thycotic, BeyondTrust, CloudAccount, or AppViewX Vault, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault.
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port number 443 (API)
- **Location from which the certificates are discovered if Certificate Managed**: Certificates are fetched by issuing a direct API call to the device.

Onboarding Palo Alto Device

To add a PaloAlto device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **PaloAlto** vendor from the left side bar. bar.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • Firewall • Panorama.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

5. Enter or select the field information in the **Credentials** section:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Expert password	Enter the password.
**: Mandatory fields*	

6. Enter or select the field information in the **Secondary device information** section as follows:

   • **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.

   • **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.

   • **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the Palo Alto Device

1. Go to (**Menu**) > **FIREWALL+** > **Device Management** > **Inventory** > **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate the device addition.

Onboarding Certificates for Palo Alto

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certificates

Discovering Certificates for Palo Alto

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Firewalls**.
Devices window	A list of all the managed firewall devices is displayed in the devices window.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to a Palo Alto Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Palo Alto

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Firewall**.
***Vendor**	From the dropdown list, select **PaloAlto**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **Profile Selection** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

Profiles will be discovered irrespective of the cert sync option selected during device addition or during an on-demand discovery.

- **The following profiles will be discovered currently in AppViewX for Palo Ato Firewall:**
  - **Shared location** - denotes a push only operation which pushes a certificate to the end device.
  - **SSL/TLS Service profile** - A pushed certificate to the device can be associated to any available SSL/TLS profile in the device.
  - **IKE Gateways** - A pushed certificate to the device can be associated to any IKE gateway where certificate was chosen as authentication type.
  - **SSL Inbound Inspection Profiles** - The pushed certificate can also be associated to a decryption rule.
  - **Authentication Profiles** - A pushed certificate can be associated with an authentication profile, typically used for authenticating users or administrators. This includes profiles configured to use client certificates or SAML authentication where a signing certificate or certificate profile is referenced.

    Note: The shared location profile will be framed by default when a device is added, but for the other profiles to be framed they have to configured in the device.

- **The following profiles will be discovered currently in AppViewX for Palo Alto Panorama:**
  - **Shared location** - denotes a push only operation which pushes a certificate to the end device. This functionality is enabled for both the shared location of Panorama and the shared location of templates.
  - **SSL/TLS Service profile** - A pushed certificate to the device can be associated to any available SSL/TLS profile in the device. Note: Profiles will be framed for SSL/TLS profiles in both Panorama and template/ template stacks.
  - **IKE Gateways** - A pushed certificate to the device can be associated to any IKE gateway where certificate was chosen as authentication type.
  - **SSL Inbound Inspection Profiles** - The pushed certificate can also be associated to a decryption rule under policies section for policy managed in a template.
  - **Authentication Profiles** - A pushed certificate can be associated with an authentication profile, typically used for authenticating users or administrators. This includes profiles configured to use client certificates or SAML authentication where a signing certificate or certificate profile is referenced.

    Note: The shared location profile will be framed by default when a device is added, but for the other profiles to be framed they have to configured in the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. To select the device(s) to which the certificate will be pushed, under **Profile Selection**, from the list of **Available Devices**, click .

   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Password	Enter the password required to access the certificate file/trust store.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.
Push to Firewall	This field appears only when Platform = Panorama. Pushing the configuration changes to the firewall devices in Panorama can be managed through this setting. The available options are: • **Not Required:** This option commits changes to Panorama only after a successful push and bind operation. It does not synchronize the chaages with the firewall. • **Push Only:** This option pushes and commits the certificates to Panorama and the firewall but it does not perform a commit after binding the certificate to the profile. • **Push and Commit:** This option pushes and binds the certificates to Panorama and the firewall profile followed by a commit operation. **Note:** Alternatively, you can provide the dropdown values in **CERT+ > Device Management > Firewall >** **(Device Settings) > Palo Alto.**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Trust Type	**Important:** Trust type is applicable only for server certificates issued by private CAs with a customized template that issues certificate to the PaloAlto device with **Key Usage** as **Certificate Signing** for certificates that have a private key. **Trust Type** defines how a firewall handles SSL/TLS traffic based on whether a certificate is trusted or untrusted. Select a trust type status from the following values: • **Forward Trust** Select this option to establish the firewall as a trusted third party (proxy) to the session between the client and the server. For **Trust Type** = **Forward Trust**, if the server's certificate is valid (trusted) and signed by a known, trusted CA (like VeriSign, DigiCert, etc.), the firewall decrypts the traffic, inspects it, and then re-encrypts it using its own certificate, which is trusted by the client due to the configured CA. • **Forward Untrust** Select this option for the firewall to notify to clients when the server certificate is signed by a CA that the firewall does not trust. For **Trust Type** = **Forward Untrust**, if the server's certificate is self-signed or from an unknown CA, the firewall may re-encrypt the traffic using an untrusted certificate, causing the client to see a warning that the connection is not secure. **Note:** If the certificate trust type was already specified when configuring the certificate on the device, then upon discovery in AppViewX, the trust type field will reflect the same value as configured in the device port.

4. Enter/Select the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

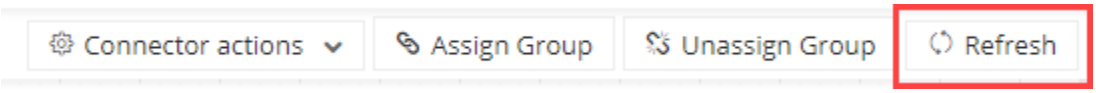
- The approval process is triggered. The current flow is based on the default policy of two-level approvals.
- A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.
   The holistic view of the selected certificate is displayed.

   Note: For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Paloalto Firewall

This section helps you troubleshoot the common problems that you might encounter while using Paloalto firewall functionalities. This guide will give more troubleshooting processes on Paloalto firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Paloalto firewall.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Unsupported Key type provided	Unsupported key type is selected.	Please select RSA or EC.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Invalid parameter for number of bits Csr generation is device failed	Selected EC bit length may not be supported by Paloalto.	Please select valid bit length supported.

Issues in Certificate Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name not given or length less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.

Issues in Backup, Push, Bind and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Exception occured while getting Api key - Invalid credentials.	Credentials may be invalid.	Provide valid credentials.
Certificate <cert name> is not a valid reference	Private key not available in the certificate or the certificate is not in the required partition to bind.	Certificate should be pushed with the private key to bind with the profile.
Creating local certificate file failed	Unable to create the folder in EXPORT_DIRECTORY.	Please check whether the user has permission to create a folder or file in EXPORT_DIRECTORY in AppViewX.
Certificate name already exists in inventory, Cannot overwrite until Overwrite is enabled in Profile connector	Certificate with the same name already exists on the device.	Please change the certificate name or enable overwrite in the application connector.
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than current time.	Only valid certificates can be pushed.

Automating CLM for CheckPoint

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
  - The username and password entered during the device onboarding process must be identical in both the Gaia Portal and the Smart Console user accounts. This ensures consistency, as the same credentials will be used for authentication in Gaia CLI and Management REST API sessions.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Admin Portal**: To read/modify the certificate used for admin portal, cat/echo commands are needed. Generic linux commands can be executed only in expert mode. **In order to switch to expert mode admin privileges has to be given in the Gaia portal for a user.**
- **HTTPS Inspection**: To read/modify inspection rules and to add server certificates, these are the permissions needed in Checkpoint Management Smart Console.
  - **Access Control** > **General** > **Access Control Objects and Settings** > **Write**.
  - **Others** > **Permissions** > **HTTPS Inspection** > **Write**.
  - **Management** > **Publish sessions without an approval** > **Write**.
  - **Management** > **Management API Login** > **Write**.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
  - If authentication relies on an external credential such as AppViewX, Thycotic, BeyondTrust, Hashicorp, and CyberArk, ensure that the hostname, FQDN, or IP address used for device communication is configured in the corresponding external credential vault.
- **Platform**: Security Management Server
- **Enable Password**: Required
- **License Check**: Not required
- **Services**
  - Admin Portal (requires SSH port)
  - HTTPS Inspection (requires https port).
- **Supported versions**: vR75.x, vR77.x, vR80.x, vR81.x
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**:
  - Certificates are fetched by issuing a direct command to the device through SSH.
  - Location in the device:
    - /web/conf/server.crt
    - /web/conf/server.key

Note: Discovering the certificates used for inbound inspection is not feasible because Checkpoint does not provide an API to retrieve the content of the certificates. Therefore, only the formation of profiles for the server certificates' shared location and the inspection policies will be done by AppViewX.

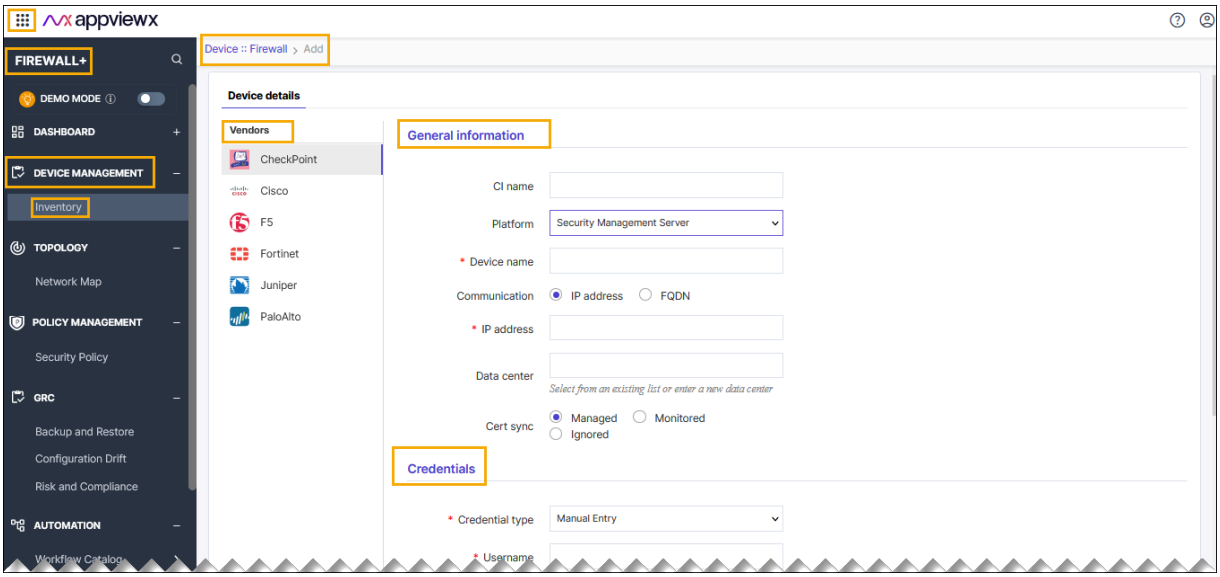
Note: For Visual Workflow action items, you will require credentials with write privilege.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding CheckPoint Device

To add a CheckPoint device:

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **CheckPoint** vendor from the left command bar



4. Enter the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • **Security Management Server** • MultiDomain Security.
***Device name**	Unique custom identifier of your device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	The data center on which the device has been hosted. Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
***Services**	Select the required services. By default **Admin Portal** is selected. The available services are, • **Admin Portal** • **HTTPS Inspection**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • If you select **HTTPS Inspection**, the HTTPS Port field becomes enabled, and inspection profiles appear in the application connector. • HTTPS supports only profile discovery, certificate push, and certificate binding.
***SSH Port**	Enter the SSH port number on the field.
***HTTPS Port**	Enter the SSH port number on the field.
**: Mandatory fields*	

5. Enter the field information in the **Credentials** section:

Field and Description Table

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the dropdown list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. To create a credential list, see Creating Credential List in the ***Platform User Guide***.
***Username**	Username for the firewall device when you select the **Manual Entry** credential type.
***Password**	Valid password for the firewall device when you select the **Manual Entry** credential type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
***Expert password**	Enter the privilege password.
**: Mandatory fields*	

6. Enter the field information in the **Secondary device information** section as follows:
   - **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
   - **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
   - **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

   Note:
   - By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
   - By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

   Note:
   - To discard the changes, click the Cancel button.

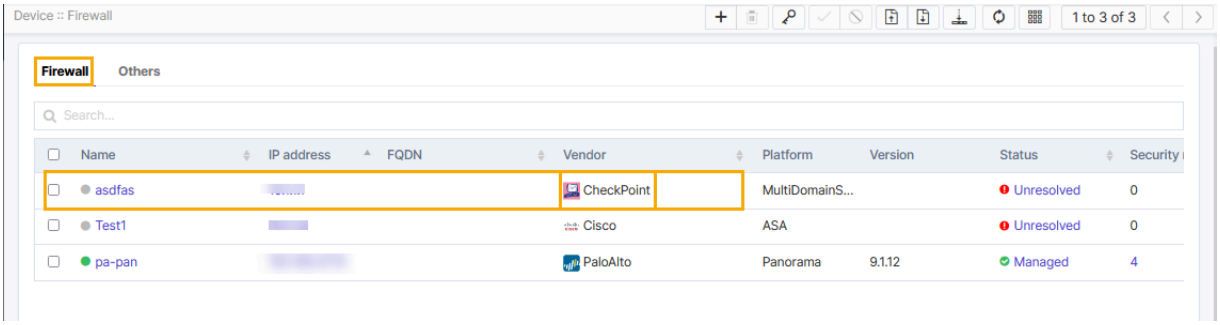
   A pop-up message is displayed as **Device added successfully**.

Validating the CheckPoint Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Onboarding Certificates for CheckPoint

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certificates.

Discovering Certificates for CheckPoint

Note: Discovering the certificates used for inbound inspection is not feasible because Checkpoint does not provide an API to retrieve the content of the certificates. Therefore, only the formation of profiles for the server certificates' shared location and the inspection policies will be done by AppViewX.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Firewalls**.
Devices window	A list of all the managed firewall devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to a CheckPoint Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for CheckPoint

1. Enter the **General Information** for the connector.

Field	Description
***Category**	From the dropdown list, select **Firewall**.
***Vendor**	From the dropdown list, select **CheckPoint**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **Profile Selection** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

Profiles will be discovered irrespective of the cert sync option selected during device addition or during an on-demand discovery.

- **Admin Portal**: The Admin portal CLM integration in AppViewX with CheckPoint is primarily designed to discover and manage the server certificate found at the file path **'/web/conf/server.crt'** in both SMS and MDS environments.

  Note: For executing linux commands, it's necessary to enter expert mode on the CheckPoint device. This is achieved using the command 'expert'. During the device addition process in AppViewX, an expert password field is provided to facilitate switching to expert mode when required.

- **HTTPS Inspection**: HTTPS Inpsection has to be enabled in services during device on-boarding to perform end-to-end automation for inspection certificates.
  - **Push Only Profile**

    Format: deviceName:HTTPSInspection:ServerCertificate

    Description: This profile is used for pushing server certificates only. It does not bind the certificates to any specific inspection rules.
  - **Push and Bind Profile**

    Format: deviceName:HTTPSInspection:InspectionLayerName:RuleNumber:RuleName

    Description: This profile is used for both pushing and binding certificates. It binds the certificates to specific inspection rules defined by the rule number and rule name.

2. To select the device(s) to which the certificate will be pushed, under **Profile Selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Password	Enter the password required to access the certificate file/trust store.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

4. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where th pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.

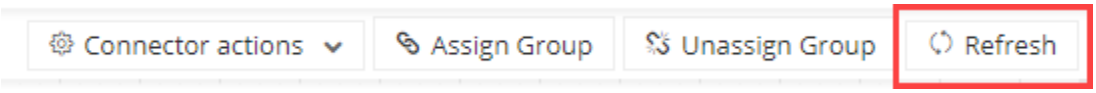
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.
   The holistic view of the selected certificate is displayed.

   Note: For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting Check point Firewall

This document helps you troubleshoot the common problems that you might encounter when using the Check point firewall functionalities. This guide will give more troubleshooting processes on Check point firewall certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with Check point firewall.

Issues when device goes to unresolved state after on-boarding

The device might have entered an unresolved state due to connectivity issues from the AppViewX installed node or CC node. In such cases, please follow the steps below:

1. Attempt to establish an SSH connection from the AppViewX installed node or CC node to the Check point server.
2. Verify if there is proper connectivity between the nodes and the Check point server.

Issues when device goes to failed state with version failure

When a device enters a failed state with version check failure, it typically indicates that the system is unable to retrieve the version information from the Check point SMS server.

1. Login to the Check point SMS server via CLI using the credentials configured in AppViewX.
2. Attempt to enter expert mode. The user should be able to switch to expert mode.
   - Verify the expert password provided during on-boarding is correct.
   - Confirm expert mode privileges are granted for the user account.
3. Once in expert mode, execute the following command: **`fwm ver`**. This command should confirm the server is indeed a Check point SMS server and display the version details of the server.
   Sample expected output:

```
This is Check Point Security Management Server R81.20 - Build 440
```

Automating CLM for F5 Devices

Prerequisites

1. Download:
   - iControl from https://community.f5.com/kb/technicalarticles/icontrol-library-for-java-with-source/279110
   - axis JAR files from https://repo1.maven.org/maven2/org/apache/axis/axis/1.4/axis-1.4.jar
   - javax.xml.soap-api-1.4.0.jar from the file library.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Copy both the JAR files to an AppViewX node as the installed user.
   - **On-prem**: Place the JAR files in the **appviewx_dependencies/external_libs/** folder within the AppViewX installation directory.
   - **SaaS**: Place the JAR files in **deps/external_libs** where the cloud connector is installed.
3. Ensure the following prerequisites are met:
   - **Version Supported**: v11.x , v12.x , v13.x, v14.x, v15.x, v16.x, v17
   - **IP Address/FQDN**: IP address or FQDN
   - **User Privilege**: { Role : Admin , bash access is required } Username /Password, Credential List AppViewx/CyberArk
   - **Enable Password**: Not applicable
   - **License Check**: Yes
   - **Services and Ports for AppViewX Communication**: 22 and 443
   - **Internet Access/Proxy if Required**: Not applicable
   - **Location from which Certificates are discovered if managed**:
     - /config/filestore/files_d/<partition>_d/certificate_d/
     - V10
     - /config/ssl/ssl.crt/
     - /config/httpd/conf/ssl.crt/
4. For SaaS, restart only the **appviewx-platform-gateway** pod in CC whereas for on-prem, restart **avx-vendors** pod.

Onboarding F5 Device

Onboarding F5 Device

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
2. Perform one of the followings:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.
   - Click **Onboard Device** in the left navigation panel.
3. In the **Device details** page, click the **F5** icon.
4. Enter or select the field information in the **General information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. For the device type **Device/Tenant**:

General information Section for "Device/Tenant" Device Type - Field and Description Table

Name	Type	Description	Validation
Device Type	Drop-down	When you select Device Type as Device/ Tenant, you will need to provide the relevant device information in the following fields.	NA
***Module**	Check box	LTM / BIG-IP DNS Module.	NA
VCMP Guest	Check box	To add a device as a vcmp guest, this checkbox should be checked.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The ipv4 address of the device.	The IP address should be a valid IPv4 format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
***Cert Sync**	Radio button	**Managed**: The certificates of the device can be managed.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		Monitored: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	
DNSSEC sync	Radio button	By default, the Ignored option is selected. If your ADC acts as an authoritative DNS server, then select the Managed option to manage the DNSSEC Zones and Keys (KSK and ZSK).	
AppViewX Group Sync	Check box	This should be enabled if the user wants to sync the devices within the device group.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

b. For the device type **Host**:

General information Section for "Host" Device Type - Field and Description Table

Name	Type	Description	Validation
Device Type	Drop-down	When you select Device Type as Host, you will need to provide the relevant device information in the following fields.	NA
Host Type	Radio button	Select any of the following host types: • vCMP Host - Enables the running of multiple virtual instances of BIG-IP software on a single physical device • rSeried Host - A host type representing the F5 rSeries hardware platform, designed for	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		high-performance application delivery and security. • Velos Partition - A logical partition on the F5 VELOS platform, allowing for the segmentation of resources and management of multiple tenants within a single VELOS chassis.	
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The ipv4 address of the device.	The IP address should be a valid IPv4 format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
**: Mandatory fields*			

c. For the device type **Controller**:

General information Section for "Controller" Device Type - Field and Description Table

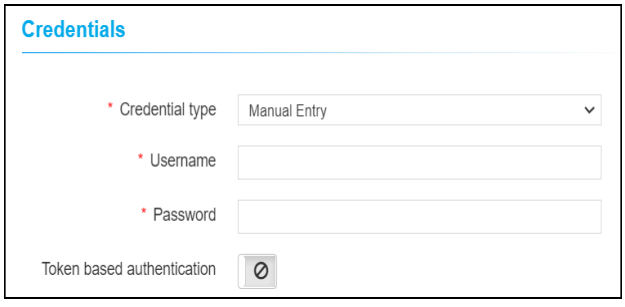
Name	Type	Description	Validation
Device Type	Drop-down	When you select Device Type as Controller, you will need to provide the relevant device information in the following fields.	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

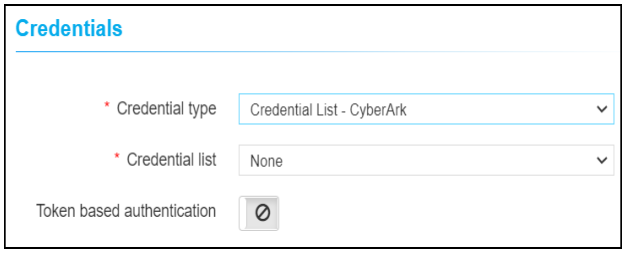
Name	Type	Description	Validation
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The ipv4 address of the device.	The IP address should be a valid IPv4 format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
**: Mandatory fields*			

5. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password. 	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Name	Type	Description	Validation
		Credential List: The user can select the credential details which are already stored in the credential inventory page. For more details on secure authentication, refer to Platform User Guide. 	
***Username**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
Token based authentication	Toggle button	To access the device REST API using token.	NA
**: Mandatory fields*			

6. Enter or select the field information in the **Secondary device information** section.

Secondary device information Section - Field and Description Table

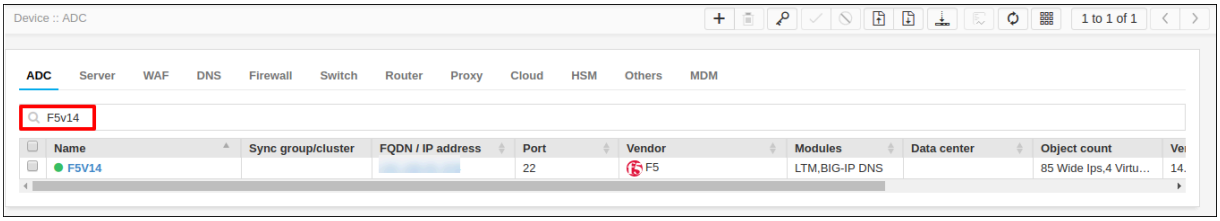
Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

7. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Validating the F5 Device Onboarding

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. From the device inventory page, search for the added F5 device name.



Onboarding Certificates for F5 Devices

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for F5 Devices

Prerequisites

- **User Permission Required**: Administrator/ Certificate Manager role
- **Terminal Access**: Advanced Shell or TMSH

Certificate discovery involves downloading certificate and key files from the device via SFTP. This method is accessible only to F5 users with Advanced Shell access. Refer to the relevant F5 article (https://my.f5.com/manage/s/article/K16621651) for detailed instructions.

For users without Advanced Shell access, SFTP attempts will fail as explained in the aforementioned F5 article. In such instances where SFTP fails, certificates and key files are retrieved using SCP.

F5 imposes restrictions on SCP access to specific paths listed in the scp.blacklist file. During discovery, encountering route limits in F5 may result in SCP download errors ("Unable to download") in the log. In such cases, two alternatives are available (and either can be chosen):

- Use REST API(s) to download the files from the device by running:

```
db.cert_metadata.update({"_id": "CERT_VENDOR_BASED_CONDITIONS"},{"$set": {map.adc_f5_discover_certs_with_rest" : "true"}});
```

- Remove the following paths accessed via AppViewX from the scp.blacklist file path accessed from AppViewX:
  - /config/filestore/files_d/
  - /config/ssl/ssl.crt/

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- /config/ssl/ssl.key/
- /config/httpd/conf/ssl.crt/
- /config/httpd/conf/ssl.key/

• Remove these paths and restart sshd based on the steps mentioned in the F5 article: https://my.f5.com/manage/s/article/K73463547

Discovering Certificates for F5 Devices

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**. The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed ADCs**.
Devices window	A list of all the managed ADC devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to a F5 Device

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for a F5 Device

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Enter the **General Information** for the ADC devices.

Field descriptions for the Certificate Details

Field	Description
***Category**	From the dropdown list, select **ADC**.
***Vendor**	From the dropdown list, select **F5**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information populated here, the **SSL profiles** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

Note: The name of this section is populated based on the **Vendor** selected.

2. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For the Web Dispatcher server, this field is enabled by default and is non-editable.
***Chain File or Bundle Name**	**Note:** This field is displayed only when **Push Root and Intermediate Certificates** is enabled. When pushing certificates to F5 devices, particularly for SSL/TLS configurations, a chain file or bundle refers to a single file that includes the entire certificate chain. Enter the chain file name in this field.

4. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system. **Note:** Overwrite option is disabled by default for Microsoft IIS.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

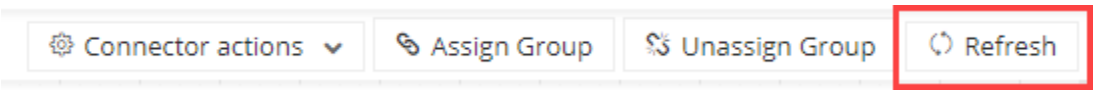
   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.
   c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

> **Note:** While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. For an existing CA connector for the certificate, hover over .

d. From the menu displayed, click **Edit**.
The certificate details are displayed.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Troubleshooting F5 WAF

This section helps you troubleshoot the common problems that you might encounter when using the F5 WAF functionalities. This guide will give more troubleshooting processes on F5 WAF certificate config fetch, discovery, CSR creation, backup, push, bind, rollback, and other actions associated with F5 WAF.

Issues in Fetch Config

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the associated error message.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovery

Error Message	Possible Cause	Possible Solution
Please provide information as required	Discovery name is not given or length is less than 2 characters.	Enter a valid name with a minimum of 2 characters.
	Interval between batches info. is missing when execution type is sequential.	Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device to discover certificates from.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
Failed to fetch partitions from the device	Partition fetch failed.	1. Check the device partitions. 2. Please check the error message associated.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.

Issues in CSR Generation

Error Message	Possible Cause	Possible Solution
Authentication failed for the device	Invalid credentials specified for the device	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
CSR Generation using HSM on this device version is not supported.	Version not supported.	Please use the supported version device to create CSR using HSM. Supported versions are v13 and v12.
1) CSR content unavailable in device	CSR content unavailable on device.	For some reasons CSR creation has failed, please check the logs to reproduce.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
2) Requested CSR is not available in device 3) Csr could not be fetched		
CSR already exists in this scope with the same Key reference name	The name is already used on the device.	Please use a different name.
Csr generation is device failed	CSR generation has failed.	CSR generation has failed. Please refer to the associated error message.
Thales HSM is not installed in the device. Please install and try again.	Thales is not installed in the device.	Please install Thales HSM and try again.
Invalid module. Please specify the valid module and try again.	Invalid module specified.	Specify a valid module and try again.
The CSR <name> was not found in the device.	CSR content is not available in the name specified.	Please check the name in the CA connector.
NetHSM private key is not available/installed in device	NetHSM private key is not available/installed in the device.	Please install NetHSM private key on the device.

Issues in F5 WAF Backup, Push, Bind, and Rollback

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
	Previous work order is in progress and not completed.	Initiate push after previous work order is finished.
	AppConnector might not be in sync.	Synchronize the appConnector and retry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state.	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Authentication failed for the device	Invalid credentials specified for the device.	Provide valid credentials for the device.
SSH connection failed	Unable to establish the SSH connection.	Please ensure that the device can be connected via SSH from AppViewX.
Invalid profile type	Specified profile type is not supported.	Please use client-SSL or server-SSL.
Certificate fetch failed	Certificate fetch failed.	Check the error message associated to know more about the problem.
Certificate already exists	Certificate is already available with the same.	Either change the name or enable overwrite in the application connector.
Key already exists	Key is already available with the same.	Either change the name of the key or enable overwrite in the application connector.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
Certificate is expired	Certificate is expired.	Push the certificate which is currently valid.
Unknown certificate algorithm	Unknown certificate algorithm.	Push the certificates only with RSA or EC.
certificate is not yet valid	Certificate valid from value is greater than the current time.	Only valid certificates only can be pushed.

Troubleshooting

User Permission Required:

- **Role:** Administrator
- **Terminal Access:** Advanced Shell or TMSH

Certificate Discovery

For discovering certificates from device, use SFTP to download certificate and key files from the device. SFTP will work only for F5 users provided with Advanced Shell access. Refer to the F5 article: https://my.f5.com/manage/s/article/K16621651

For Users without Advanced Shell access, SFTP will fail as stated in the above F5 article & in case of SFTP failure, try to download certificate and key files from the device using SCP.

F5 devices enforce **security restrictions** that limit access to specific directories via **SCP**. These restricted paths are defined in the `scp.blacklist` file on the device.

During certificate discovery, if these path restrictions are encountered, AppViewX may log an error such as *Unable to download* when attempting to retrieve files through SCP.

In such cases, you can proceed with either of the following alternatives to resolve the issue:

- REST API(s) can be used to download the files from device. To enable REST API(s) for downloading files, run:

```
db.cert_metadata.update({"_id": "CERT_VENDOR_BASED_CONDITIONS"},{"$set": {
"map.adc_f5_discover_certs_with_rest" : "true"}});
```

- Remove particular paths accessed via AppViewX from the scp.blacklist file.

Paths accessed from AppViewX

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- “/config/filestore/files_d/”
- “/config/ssl/ssl.crt/”
- “/config/ssl/ssl.key/”
- “/config/httpd/conf/ssl.crt/”
- “/config/httpd/conf/ssl.key/

Remove these paths and restart sshd based on the steps mentioned in the F5 article: https://my.f5.com/manage/s/article/K73463547

Note: If user has been provided with Advanced Shell access, both SFTP and SCP will work without any modification in device configuration or DB query execution.

CLI command to check whether SFTP is working from AppViewX to device:

Run the SFTP command from AppViewX CLI -> sftp < username >@ (Ex: sftp admin@192.168.41.2)

CLI command to check whether SCP works between device and AppViewX

1. Open an SSH connection to the device -> ssh username@
2. Run bash command.
3. Change the directory to any one of the certificate location

   cd /config/filestore/files_d/Common_d/certificate_d/

4. Run ls command and copy any one of the certificate file name.
5. Try SCP for the file copied to AppViewX location > scp <file_name_with_location><appviewx_user_name>@<appviewx_ip>:<appviewx_location>

   Example:

   ```
   "/config/filestore/files_d/Common_d/certificate_d/:Common:Xecure.crt_67510_4" appviewx@192.168.220.129:/home/appviewx/)
   ```

Certificate Push

During certificate push, the file will be copied from AppViewX to the F5 device certificate location; If push fails with the error, *Unable to upload file using SCP*, it is because of the F5 device's SCP constraints. You can use any of the solution approaches:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The certificate file must be copied to an **SCP-allowed directory** on the F5 device. From there, it will be relocated internally to the appropriate certificate location.

  To enable this behavior, run the following database query, specifying any SCP-permitted path on the F5 device.

```
db.cert_metadata.update({_id:"CERT_VENDOR_BASED_CONDITIONS"},{"$set":{"map.a
dc_f5_file_upload_path":"/config/"}});
```

- Remove certificate path from the scp.blacklist file mentioned above in the solution approach of discovery.

F5 Device Communication

- Certificate discovery, push and bind functionalities in AppViewX communicates with F5 using iControl SOAP methods.
- When the F5 device uses an HTTPS port other than **443**, or if **iControl method failures** occur, AppViewX should communicate with the device through **REST API-based integration**.
- To enable the REST based communication to F5 device, run the below DB query in AppViewX DB:

```
db.cert_metadata.update({"_id": "CERT_VENDOR_BASED_CONDITIONS"},{"$set": {
"map.adc_f5_rest_enabled":"true"}})
```

Automating CLM for Citrix Devices

Prerequisites

Prerequisites for Managing Citrix devices on AppViewX are:

- **Version Supported**: V11.x, v12.x, v13.x, and 14.x
- **IP Address/FQDN**: IP address and FQDN
- **User Privilege**: [Role : Admin , bash access is required] Username /Password, Credential List AppViewx/CyberArk.
- **Enable Password**: Not applicable
- **License Check**: Yes
- **Services and Ports for AppViewX Communication**:
  - Outbound Access from AppViewX for SSH and HTTPS service (Default/Custom Port Information) is required.
  - Outbound access to port 5514 is required for Citrix Device to forward the Syslog to AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Internet Access/Proxy if Required**: Not applicable for local devices. But required, if the device needs be accessed with Public IP address.
- Required Command Policy:

```
((show cs vserver))|((show lb vserver))|((show ns partition))|
((show ssl certKey).*)|((show ssl vserver).*)|((add audit syslogAction).*)|(
(add audit syslogPolicy).*)|((bind system global).*)|((logout))|((save ns config))|
((show HA node))|((show audit syslogAction))|((show cs policy))|((show gslb service))|(
(show gslb site))|((show gslb vserver))|((show ns feature))|((show ns hardware))|(
(show ns hostName))|((show ns license))| ((show ns runningConfig))|((show ns version))|(
(show server))|((show service))|((show serviceGroup))|
((stat interface))|((stat lb vserver descending))|((stat ns))|((stat service))|
((stat system))|((switch ns partition).*)|((shell))|((add ssl certKey).*)|
((bind ssl vserver).*)|((sftp-server))|((link ssl certkey).*)|((show  ip -type).*)|
((sftp-server))|((link ssl certkey).*)|((unbind ssl vserver ).*)|((update ssl certKey).*)|
((set ssl vserver).*)|((show system file).*)|((add system file).*)|((rm system file).*)|
(^show\s+ns\s+\S+)|(^show\s+ns\s+\S+\s+.*)
```

Web Browser Requirement

Browsers	Version
Internet Explorer	v11.0.9600.18817 or later
Firefox	118.0.1 (64-bit) or later
Google Chrome	117.0.5938.134 (Official Build) (64-bit) or later

ACF Permission

Ensure the following ACF permission is available to add and manage devices:

- ADC > Inventory > Add / Modify
- ADC > Device group > Add / Modify

You can check this under any of the following menus:

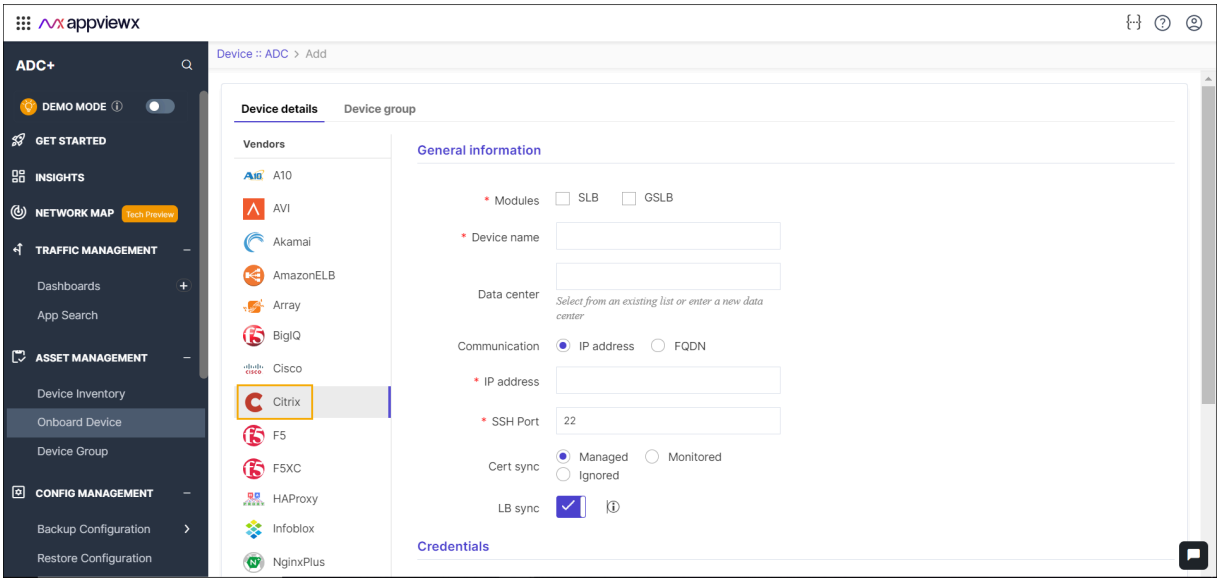
- **Old menu**: menu > Accounts > Role
- **New menu**: menu > Platform > IDENTITY > Role

To associate ACF permissions with a role, see Platform User Guide.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

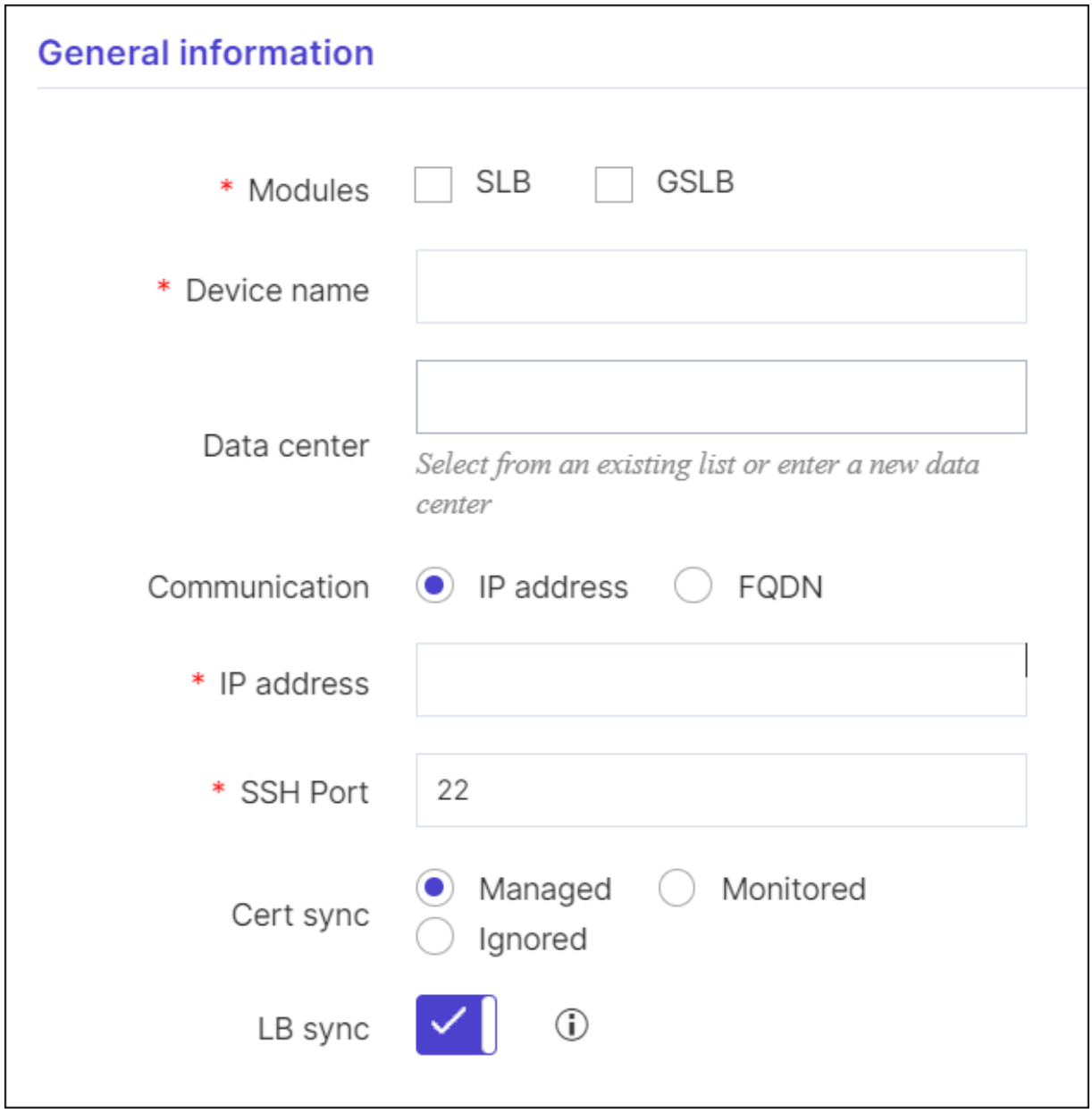
Onboarding Citrix Device

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
2. Perform one of the followings:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.
   - Click **Onboard Device** in the left navigation panel.
3. In the **Device details** page, select **Citrix** from the left sidebar.



4. Enter or select the field information in the **General information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



General information Section - Field and Description Table

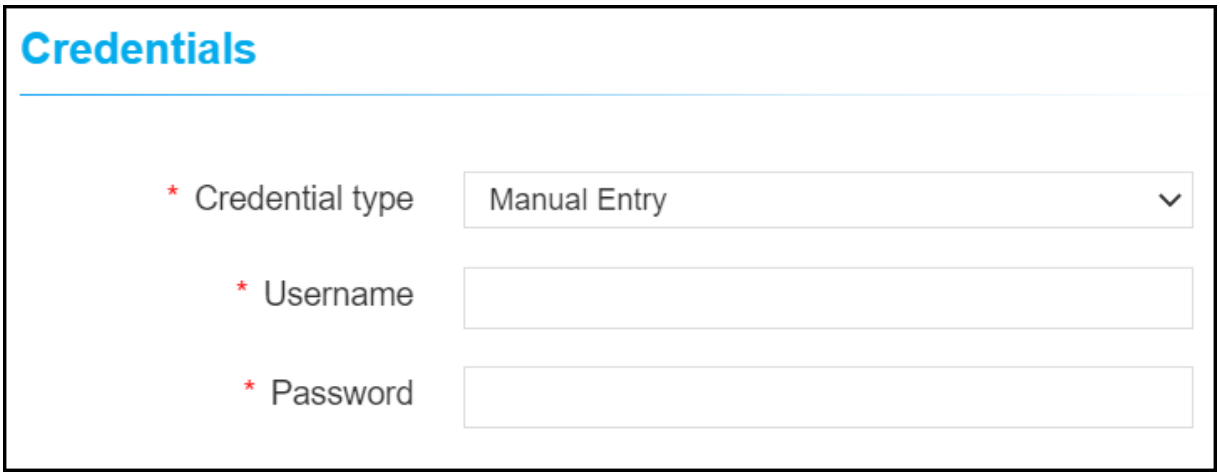
Name	Type	Description	Validation
***Module**	Check box	SLB / GSLB Module.	NA
***Device name**	Text	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

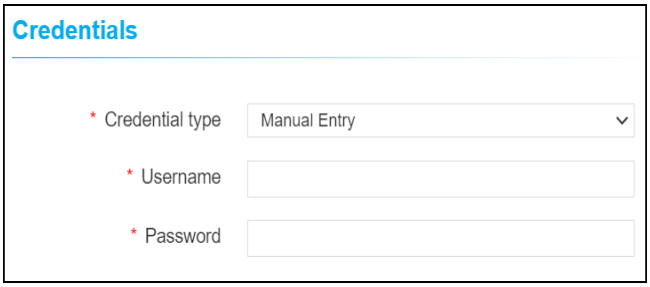
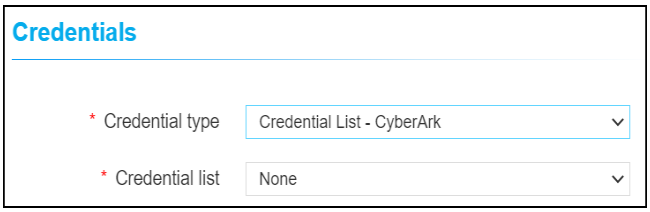
Name	Type	Description	Validation
Data center	Text	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
***Communication**	Radio button	Devices can be accessed using an IP address or FQDN.	NA
***IP Address**	Text	The IPv4 address of the device.	The IP address should be in the right format.
***FQDN**	Text	The FQDN of the device.	the FQDN should be in a valid format.
***SSH Port**	Text	Communication port of the device.	Numbers only.
***Cert Sync**	Radio button	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	NA
LB Sync	Checkbox	By default, this option is enabled to discover and manage the load balancer configurations. If not required, you can disable this option.	
**: Mandatory fields*			

5. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

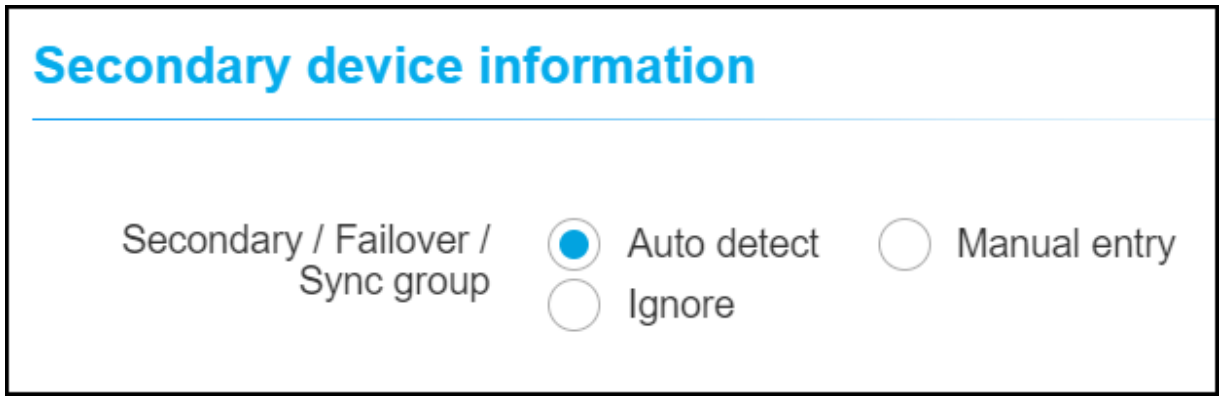


Credentials Section - Field and Description Table

Name	Type	Description	Validation
***Credential type**	Dropdown	**Manual entry**: The user should enter the username and password.  **Credential List**: The user can select the credential details which are already stored in the credential inventory page. 	NA
***Username**	Text	The user name of the device.	NA
***Password**	Text	The password of the device.	NA
**: Mandatory fields*			

6. Enter or select the field information in the **Secondary device information** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Secondary device information Section - Field and Description Table

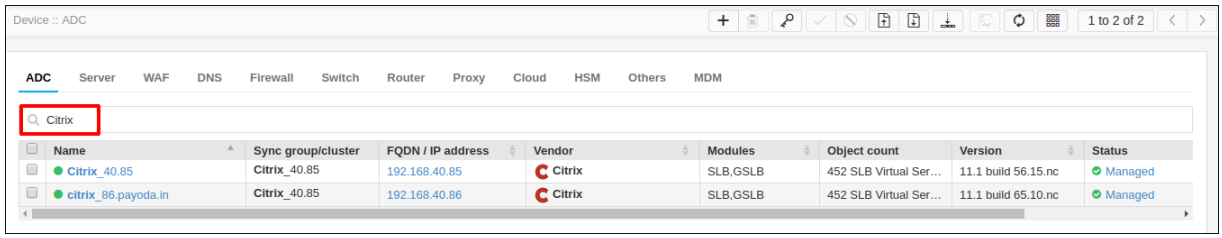
Name	Type	Description	Validation
Secondary device information	Radio button	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

7. Click **Save**.

Validating the Citrix Device Onboarding

After adding the device, you can validate the device by searching device in the device inventory.

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



Onboarding Certificates for Citrix Devices

There are two ways you can onboard certificates in AppViewX:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

• Via certificate discovery, for existing certificates
• Via certificate enrollment, for new certifcates

Discovering Certificates for Citrix Devices

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed ADCs**.
Devices window	A list of all the managed ADC devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.

Enrolling Certificates

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regenaration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given below. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions below.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

> **Note:** For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	From the dropdown list, select the Subject Alternative Name category for the certificate being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	In the corresponding field(s) displayed for the selection made, enter the required values. **Note:** • Multiple values must be separated by a comma. • After enrollment, the cumulative count of SANs is displayed in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** For renewal of the certificate being enrolled, country name is required.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you've uploaded multiple attachments, use the **Search** field to find the required one.
*: Mandatory fields	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**. **Note:** This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

    Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

Client certificate enrollment refers to the process of creating a digital ID for an individual/device for authentication/encryption purposes. It follows the same process as a server certificate.

Note: These certificates cannot be hosted on clients.

To enroll a client certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled. **Note:** This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the references section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the references section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given. To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given below. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If Regenerate Automatically field, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page. Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

References

- Creating and managing certificate V3 extension profiles in Futurex
- Creating and managing approval groups in Futurex

Pushing Certificates to a Citrix Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for a Citrix Device

1. Enter the **General Information** for the ADC devices.

Field descriptions for the Certificate Details

Field	Description
***Category**	From the dropdown list, select **ADC**.
***Vendor**	From the dropdown list, select **Citrix**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.
**: Mandatory fields*	

Based on the information populated here, the **SSL profiles** section is populated with the list of available devices for the specified vendor that are already onboarded in AppViewX.

Note: The name of this section is populated based on the **Vendor** selected.

2. To select the device(s) to which the certificate will be pushed, under **SSL profiles**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
3. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***Certificate key pair name**	The name with which the certificate-key pair will be created in the device with above certificate and key.
Enable SNI Push for Certificate	If enabled, certificate will be enabled with SNI while associating to the virtual server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Enable SNI in Virtual Server	If enabled, SNI will be enabled in Virtual Server
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For the Web Dispatcher server, this field is enabled by default and is non-editable.
***Intermediate File Name 1**	Enter the intermediate file name.
***CA File Name**	Enter the CA file name.
**: Mandatory fields*	

4. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.
**: Mandatory fields*	

5. Click **Save**.
   The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

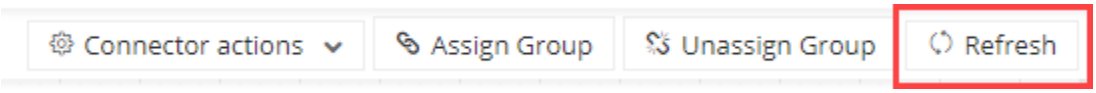
   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
    a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
    The **Group** page is displayed.
    b. From the **Name** field, select the required certificate group.
    The **Group : Modify : <group name>** page is displayed.
    c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
    d. Click **Update**.
2. To enable auto push for the certificate connector:
    a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
    To add an application connector, follow the instructions given here.
    b. From the menu displayed, click **Edit**.
    The **Edit Application Connector** pop-up is displayed.
    c. Select the **Push automatically** checkbox.

    > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

    d. Click **Save**.
    The holistic view of the selected certificate is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

> **Note:** While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:
    a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
    The **Group** page is displayed.
    b. From the **Name** field, select the required certificate group.
    The **Group : Modify : <group name>** page is displayed.
    c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.
    d. Click **Update**.
2. To enable auto renewal for the certificate connector:
    a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
    The **Server Certificate** inventory is displayed.
    b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
    The holistic view of the selected certificate is displayed.
    c. For an existing CA connector for the certificate, hover over .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

d. From the menu displayed, click **Edit**.
The certificate details are displayed.

e. Under **CA Details**, turn on the **Renew Automatically** toggle.

f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

g. Click **Update**.
The holistic view of the selected certificate is displayed.

> **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Automating CLM for AWS Resources

Amazon Web Services (AWS) is a comprehensive and widely adopted cloud platform provided by Amazon. It offers a wide array of services such as computing power, storage options, networking, databases, and more, allowing businesses and individuals to build, deploy, and manage applications and infrastructure without having to invest in physical hardware.

This section will guide you through the process of integrating AWS with AppViewX, providing detailed steps, configuration guidelines, and automation techniques for the following services:

- With ACM Integration
- With IAM Integration
- With ELB Integration
- With CloudFront Integration
- With EC2 Integration

With ACM Integration

This document will guide you through the process of integrating the ACM AWS service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) is a service provided by Amazon Web Services that simplifies the process of provisioning, managing, and deploying SSL/TLS certificates for use with AWS services and your internal connected resources.

Onboarding AWS Resources with ACM Integration in AppViewX

Onboarding AWS Standalone Accounts in AppViewX

A standalone AWS account operates independently with its own set of resources and is not connected to any other AWS accounts.

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important:

- AWS standalone device migration is supported only from the following versions of CERT + SaaS: v2020.1, v2020.2, v2020.3 - v2020.3 FP7. The following prerequisites are also applicable to only these versions.
- AWS device migration is not supported from the following versions of CERT+ SaaS: v2012.x, v2019.x, and v2021.x. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Note:

- For customers migrating from versions 20.1.x, 20.2.x, and 20.3.6, AppViewX recommends that you delete the following before migration:
  - All of their Amazon CA settings
  - Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).
- For customers migrating from version v2020.3.10 (mandatory):
  - Delete all of their Amazon CA settings before migration.
  - Trigger config fetch for all of their cloud accounts after migration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The following actions have to be performed for the standalone AWS cloud accounts migrated from the above listed versions to version v2022.1 FP1:

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.

   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.

   The **Device :: Cloud** page is displayed.
3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

   Troubleshooting: If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.
4. From the top-right corner of the **Device :: Coud** page, click the (**Fetch config**).

   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

Note: For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Before migration
  1. Merge permissions from all individual buckets into any one S3 bucket.
- After migration
  1. Select a migrated standalone account from the **Device :: Cloud** page.

     The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
  2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
  3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
  4. Click **Add**.
  5. Click **Save**.

     Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

Permissions Required for Onboarding Standalone Accounts

IAM Prerequisites for Discovering and Managing SSL Certificates in ACM

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "acm:DescribeCertificate",
            "acm:RequestCertificate",
            "acm:GetCertificate",
            "ec2:DescribeRegions",
            "acm:ListCertificates",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate"
         ],
         "Resource": "*"
      }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  ]
}
```

Onboarding AWS Standalone Accounts with ACM Integration

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, select **Standalone**.
Account name*	Enter the customer's unique AWS account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
Account number*	Enter the customer's AWS account number.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account).
Access key*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret key*	Enter the secret key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	According to the type of the new cloud device being added, select the corresponding Amazon Cloud Service for the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Service region*	Service regions are regions that are supported by the selected service. From the dropdown list, select the service regions that should be scanned for certificates. **Note:** To be able to fetch and select from the available regions, ensure that the credentials have been provided in the **Credentials** section.
CA Operation Mode*	**Note:** This field is displayed only when the **Amazon Private CA** service is selected. From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • **ACM** • **PCA**
S3 Bucket*	**Note:** This field is displayed only when the **PCA** CA operation mode is selected. Enter the S3 bucket name.
Discovery Certificate	**Note:** This field is displayed only when one/both of the CA operation modes are selected. To enable instance certificate discovery at the time of device addition, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

Onboarding AWS Cross Accounts in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

This section of the documentation will guide you through the process of onboarding an AWS cross account, for both discovery types, in AppViewX. In AWS, cross-account discovery can be set up in two ways:

- **Organization-based**: A centralized discovery mechanism that automatically finds and accesses resources across accounts in your AWS Organization using built-in trust and roles
- **IAM Policy-based**: A more flexible discovery mechanism that allows to connect to only the required accounts by manually configuring roles and permissions

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Prerequisites for Onboarding a AWS Cross Account in AppViewX

- Ensure that the following configurations are done on the AWS Management Console:
  - In your AWS master account:
    1. Create an IAM user in the AWS master account.
    2. Generate user identity.
    3. Attach policies to the created user.

       For the AWS IAM permissions to be added for the master account, click here.
  - In your AWS child account:
    1. Create a role in the child account in AWS.
    2. Attach policies to the created role.

       For the AWS IAM permissions to be added for the child account, click here.
    3. Create an EC2 role. This will be used to manage the existing EC2 instance in the AppViewX device inventory.
    4. Attach policies to the EC2 role.

       For the AWS IAM permissions for the EC2 policy, click here.

       For the AWS IAM permissions for the EC2 role, click here.

Note: For detailed instructions, you can access the corresponding AWS documentation using the references given here.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

> **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

- Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Onboarding a Cross Account in AppViewX for Organization-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	To onboard a cross account for organization-based discovery: a. Select **Organization Based Discovery**. The **Organization based Discovery** dialog box is displayed. b. Enter/Select the details required to configure organization-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Policy Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the ACM service component(s) required for the CLM operations. Depending on the service component(s) selected, additional fields are displayed. The instructions for these fields are covered in the subsequent steps.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **ACM Certificate Authority Service** section.

> **Note:** This section is displayed only when one or both **ACM** services are selected from the **Services** dropdown list.

Field description for the ACM Certificate Authority Service

Field	Description
Role Setting Preference*	**Note:** This field is displayed only when both auto discovery modes (**Organization Based Discovery** and **IAM Policy Based Discovery**) are selected. From the dropdown list, select one of the following options: • **Organization Based Discovery** • **IAM Policy Based Discovery**
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle.
**: Mandatory fields*	

9. Enter/Select the required details in the **ACM Private CA** section.

> **Note:** This section is displayed only when the **ACM (Amazon Private CA)** service is selected for a **Cross or Federated** account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the ACM Private CA section

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>CA Operation Mode*</td><td>From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority:
• ACM
• PCA</td></tr>
<tr><td>S3 Bucket*</td><td>NOTE: This field is displayed only when the PCA operation mode is selected.
a. Enter the S3 bucket name.
b. Click .
The ARN Advanced Settings action pane is displayed.
c. In the ARN Advanced Settings action pane, enter the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming</td></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.
Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.
Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:

i. In the Enter Key field, enter a key for the key-value pair.

ii. In the Enter Value field, enter a value for the key-value pair.

iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
d. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

10. To add the new device to the cloud device inventory, click **Add**.
11. Click **Save**.

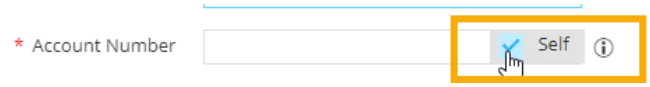
    The added device is listed in the outer inventory on the **Device :: Cloud** page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.
   The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

> **Note:**
> - If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
> - Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding a Cross Account in AppViewX for IAM Policy-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	To onboard a cross account for IAM policy-based discovery: a. Select **Policy Based Discovery**. The **Policy based Discovery** dialog box is displayed. b. Enter/Select the details required to configure IAM policy-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Organization Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the ACM service component(s) required for the CLM operations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Depending on the service component(s) selected, additional fields are displayed. The instructions for these fields are covered in the subsequent steps.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **ACM Certificate Authority Service** section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: This section is displayed only when one or both **ACM** services are selected from the **Services** dropdown list.

Field description for the ACM Certificate Authority Service

Field	Description
Role Setting Preference*	**Note:** This field is displayed only when both auto discovery modes (**Organization Based Discovery** and **IAM Policy Based Discovery**) are selected. From the dropdown list, select one of the following options: • **Organization Based Discovery** • **IAM Policy Based Discovery**
Route53 Zone Auto Approval	To support DNS validation as an automatic process, enable this toggle.
**: Mandatory fields*	

9. Enter/Select the required details in the **ACM Private CA** section.

Note: This section is displayed only when the **ACM (Amazon Private CA)** service is selected for a **Cross or Federated** account.

Field description for the ACM Private CA section

Field	Description
CA Operation Mode*	From the following options, select one/both operation mode(s) for discovering all the certificates enrolled by the Private Certificate Authority: • ACM • PCA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>S3 Bucket*</td><td>
NOTE: This field is displayed only when the PCA operation mode is selected.

a. Enter the S3 bucket name.

b. Click .

The ARN Advanced Settings action pane is displayed.

c. In the ARN Advanced Settings action pane, enter the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming</td></tr>
<tr><td>Role Session name</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:

• Minimum: 900 seconds (15 minutes)

• Maximum: 129,600 seconds (36 hours)

Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:

i. In the Enter Key field, enter a key for the key-value pair.

ii. In the Enter Value field, enter a value for the key-value pair.

iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
d. Click Apply.
</td></tr>
<tr><td>Discover Certificate</td><td>To enable instant certificate discovery at the time of device addition, select this checkbox.</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

10. To add the new device to the cloud device inventory, click **Add**.

> **Tip:** To select multiple services for a device, after you click **Add**, go back to the **Services** dropdown list and select the next service you want to enable for the device. Enter/select the rest of the details and click **Add**. Repeat this process for as many services you want to enable for the new device. The table is populated with a separate entry for each service.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Details of the child accounts for the added master account are displayed in the inner inventory table at the bottom of the page. The details captured in the inner inventory are explained here.
- Details of the master account are listed on the **CERT+** > **Administration** > **Certificate Authority** > **<Selected CA>** page.

> **Note:** For a public Certificate Authority, only the child account details are listed on the **CERT +** > **Administration** > **Certificate Authority** > **Amazon** > **ACM CA** page. There is no inner inventory for a public certificate authority.

11. To add the new device to the cloud device inventory, click **Add**.
12. Click **Save**.
    The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.
   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

> **Note:**
> - If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
> - Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Field	Description
Account Name	Name of the account to which the cloud device belongs

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

AWS IAM Prerequisites for Master Account

Permissions for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:GetUserPolicy",
      "iam:ListGroupsForUser",
      "iam:ListGroupPolicies",
      "iam:ListAttachedUserPolicies",
      "iam:ListAttachedGroupPolicies",
      "iam:ListUserPolicies",
      "iam:GetGroupPolicy",
      "iam:GetUser"
    ],
    "Resource": "*"
  }
 ]
}
```

Permissions for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  ]
}
```

Permissions for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": [
    "arn:aws:iam::<child account 1>:role/<Assume-role>",
    "arn:aws:iam::<child account 2>:role/< Assume-role>",
    "arn:aws:iam::<child account 3>:role/< Assume-role>"
   ]
  }
 ]
}
```

Permissions for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

```
{
 "Version": "2012-10-17",
 "Statement": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  {
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "sts:AssumeRole"
    ],
    "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

Permissions for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::<child-account>:role/AppViewX-S3-Bucket-Access"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

AWS IAM Prerequisites for Child Account

Permissions for Establishing a Trust Relationship in Child Accounts

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::master-account-number:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    }
  ]
}
```

Permissions for Discovering and Managing SSL Certificates in ACM

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "acm:DescribeCertificate",
                "acm:RequestCertificate",
                "acm:GetCertificate",
                "ec2:DescribeRegions",
                "acm:ListCertificates",
                "acm:ImportCertificate",
                "acm:AddTagsToCertificate",
                "acm:ListTagsForCertificate",
                "acm:RemoveTagsFromCertificate"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions for Discovering and Managing Private CA Certificates

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "acm:DescribeCertificate",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
                "acm:RequestCertificate",
                "acm:GetCertificate",
                "acm:RenewCertificate",
                "ec2:DescribeRegions",
                "acm:ListCertificates",
                "acm:ImportCertificate",
                "acm:AddTagsToCertificate",
                "acm:ListTagsForCertificate",
                "acm:RemoveTagsFromCertificate",
                "acm-pca:CreateCertificateAuthorityAuditReport",
  "acm-pca:DescribeCertificateAuthorityAuditReport,
  "acm-pca:GetCertificate",
  "acm-pca:ListCertificateAuthorities",
  "acm-pca:IssueCertificate",
  "acm-pca:RevokeCertificate",
  "s3:GetBucketLocation",
  "s3:GetObject"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions for Managing SSM Permissions for the EC2 Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ec2:DescribeInstances",
  "s3:ListAllMyBuckets",
  "ssm:DescribeInstanceInformation",
  "ssm:GetDocument",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
          ],
          "Resource": "*"
      }
   ]
}
```

Permissions for Managing SSM Permissions for EC2 Role

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "ssm:DescribeDocument",
            "ec2messages:GetEndpoint",
            "ec2messages:GetMessages",
            "ssmmessages:OpenControlChannel",
            "ec2messages:DeleteMessage",
            "ssm:UpdateInstanceInformation",
            "ec2messages:FailMessage",
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
         ],
         "Resource": "*",
         "Effect": "Allow"
      },
      {
         "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Onboarding Certificates for AWS Resources in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for AWS Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)
***Select Account View**	**Note:** This field is displayed only when you've selected **Account type** = **Cross account sign-in**. From the given options, select one to specify if the discovery will be performed for the master account or for the child accounts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Select Filter Type**	**Note:** This field is enabled when: • • **Account type** = **Stand-alone account sign-in** • **Account type** = **Cross account sign-in** AND **Select Account View** = **Child Account**. From the following options, select one to specify how the discovery results should be filtered: • **Account View** • **Service View**
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are listed in the certificate inventory.

Enrolling Certificates

Enrolling Server Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

> **Note:** For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to AWS Resources with ACM Integration

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for AWS Resources with ACM Integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **AWS**.
Service Types	From the dropdown list, **ACM**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Certificate ARN	This field is displayed when **Certificate Location** = **ACM**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The ARN (Amazon Resource Name) is a unique identifier assigned to each certificate that is managed by ACM. It is used to reference the certificate in API calls, policies, and so on. In this field, enter the ARN of the certificate to be pushed.
***Certificate File Name**	In this field, enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For AWS, this field is enabled by default and is non-editable.

5. Enter the **Certificate Tags**.
   A certificate tag is a label that you can assign to a certificate. To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

   To enter the certificate tags:

   a. **Enter Key** and **Enter Value**, in the respective fields, for the tag.

   b. Click **Add**.
      The tag, as a key-value pair, is listed in the table shown below the fields.

6. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.
Post - Push Script File Name	Enter the file name of the post push script.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.

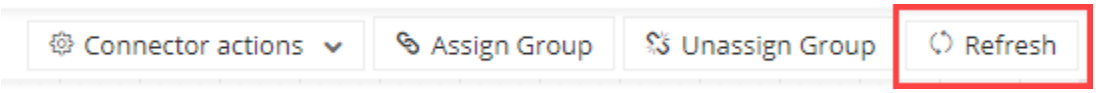
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The approval process is triggered. The current flow is based on the default policy of two-level approvals.
- A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
   The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Troubleshooting for AWS ACM

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ACM & IAM service like server addition using AppViewX, fetch, certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Server Addition using AppViewX GUI

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	Provided credential is invalid.	1. Provide valid Access Key. 2. Provide valid Secret Key.
Provide valid account name	Account name can be duplicate or not as per standard.	1. Provide unique name for account name. 2. Account name can be alphanumeric and can also have period (.) in it.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Details Incorrect	Provide mandatory fields.	Enter mandatory fields like 1. Account Number 2. Access Key 3. Secret Key 4. Data Center 5. Services 6. Regions

Issues in Fetch Regions

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	The provided credential is invalid.	1. Provide valid Access Key. 2. Provide a valid Secret key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovery in ACM

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device from which to discover certificates.

Issues in Push and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, such as in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	Userdoes not have required permissions to push to the device.	Retry after getting the access for required action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.

References

- Create an IAM user in your AWS account.
- Create access keys for the root user.
- Create IAM policies using the JSON editor.
- Accessing member accounts.
- Using IAM roles for Amazon EC2 instances.
- Define custom IAM permissions for customer managed policies.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

With IAM Integration

This document will guide you through the process of integrating the IAM AWS service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

IAM (Identity and Access Management)

IAM (Identity and Access Management) is a web service that helps you securely control access to AWS resources. IAM enables you to manage users, groups, roles, and their associated permissions to ensure that the right individuals and services have the appropriate access to your AWS resources.

Onboarding AWS Resources with IAM Integration in AppViewX

Onboarding AWS Standalone Accounts in AppViewX

A standalone AWS account operates independently with its own set of resources and is not connected to any other AWS accounts.

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important:

- AWS standalone device migration is supported only from the following versions of CERT + SaaS: v2020.1, v2020.2, v2020.3 - v2020.3 FP7. The following prerequisites are also applicable to only these versions.
- AWS device migration is not supported from the following versions of CERT+ SaaS: v2012.x, v2019.x, and v2021.x. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- For customers migrating from versions 20.1.x, 20.2.x, and 20.3.6, AppViewX recommends that you delete the following before migration:
  - All of their Amazon CA settings
  - Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).
- For customers migrating from version v2020.3.10 (mandatory):
  - Delete all of their Amazon CA settings before migration.
  - Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the standalone AWS cloud accounts migrated from the above listed versions to version v2022.1 FP1:

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.

   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.

   The **Device :: Cloud** page is displayed.
3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

   Troubleshooting: If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.
4. From the top-right corner of the **Device :: Coud** page, click the (**Fetch config**).

   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

Note: For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

- Before migration
  1. Merge permissions from all individual buckets into any one S3 bucket.
- After migration
  1. Select a migrated standalone account from the **Device :: Cloud** page.

     The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
  2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
  3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
  4. Click **Add**.
  5. Click **Save**.

     Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

Permissions Required for Onboarding Standalone Accounts

IAM Prerequisites for Discovering and Managing Certificates in IAM

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "iam:ListServerCertificates",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    }
  ]
}
```

Onboarding AWS Standalone Accounts with IAM Integration

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, select **Standalone**.
Account name*	Enter the customer's unique AWS account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Account number*	Enter the customer's AWS account number.
Account Description	Enter a description of the device to be added.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account).
Access Key ID*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret Access Key*	Enter the secret key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	From the dropdown list, select **IAM** > **Identity & Access Management (IAM)** .
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

Onboarding AWS Cross Accounts in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

This section of the documentation will guide you through the process of onboarding an AWS cross account, for both discovery types, in AppViewX. In AWS, cross-account discovery can be set up in two ways:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Organization-based**: A centralized discovery mechanism that automatically finds and accesses resources across accounts in your AWS Organization using built-in trust and roles
- **IAM Policy-based**: A more flexible discovery mechanism that allows to connect to only the required accounts by manually configuring roles and permissions

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Prerequisites for Onboarding a AWS Cross Account in AppViewX

- Ensure that the following configurations are done on the AWS Management Console:
  - In your AWS master account:
    1. Create an IAM user in the AWS master account.
    2. Generate user identity.
    3. Attach policies to the created user.

       For the AWS IAM permissions to be added for the master account, click here.
  - In your AWS child account:
    1. Create a role in the child account in AWS.
    2. Attach policies to the created role.

       For the AWS IAM permissions to be added for the child account, click here.
    3. Create an EC2 role. This will be used to manage the existing EC2 instance in the AppViewX device inventory.
    4. Attach policies to the EC2 role.

       For the AWS IAM permissions for the EC2 policy, click here.

       For the AWS IAM permissions for the EC2 role, click here.

> **Note:** For detailed instructions, you can access the corresponding AWS documentation using the references given here.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

> **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

- Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Onboarding a Cross Account in AppViewX for Organization-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	To onboard a cross account for organization-based discovery: a. Select **Organization Based Discovery**. The **Organization based Discovery** dialog box is displayed. b. Enter/Select the details required to configure organization-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Policy Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the IAM service component for the CLM operations.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

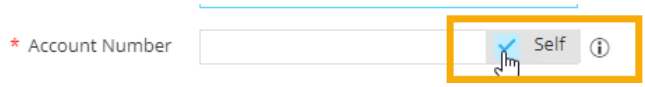
Field	Description
	If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. To add the new device to the cloud device inventory, click **Add**.
9. Click **Save**.
   The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

Note: This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Onboarding a Cross Account in AppViewX for IAM Policy-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
: Mandatory fields	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	To onboard a cross account for IAM policy-based discovery: a. Select **Policy Based Discovery**. The **Policy based Discovery** dialog box is displayed. b. Enter/Select the details required to configure IAM policy-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Organization Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the IAM service component for the CLM operations.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. To add the new device to the cloud device inventory, click **Add**.
9. Click **Save**.
   The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.

   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
• In-Progress: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is In-Progress till the resource discovery status for all individual entities is Completed.

Note: This is possible only when the account is in the Managed state.

• Completed: Resource discovery by AppViewX in the customer's AWS environment is complete.

Note: This is possible only when the account is in the Managed state.

Note:
• Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting.
• The resource discovery status of all entities mapped to the account should be Completed.

• Not Applicable: The resource discovery status is set to Not Applicable:
• when Status = Failed or Resolved,
• for ACM and ELB resources,
• for all existing devices and child accounts as part of data migration.
</td></tr>
<tr><td>Cert Discovery Status</td><td>
Note: Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to Not Applicable.

This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values:

• Not started: Certificate discovery for the entity is yet to begin

Note: At this point, the resource discovery status of the associated account can be Not started, In-Progress, or Completed.
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

AWS IAM Prerequisites for Master Account

Permissions for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:GetUserPolicy",
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListAttachedGroupPolicies",
    "iam:ListUserPolicies",
    "iam:GetGroupPolicy",
    "iam:GetUser"
   ],
   "Resource": "*"
  }
 ]
}
```

Permissions for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "organizations:List*"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": [
    "arn:aws:iam::<child account 1>:role/<Assume-role>",
    "arn:aws:iam::<child account 2>:role/< Assume-role>",
    "arn:aws:iam::<child account 3>:role/< Assume-role>"
   ]
  }
 ]
}
```

Permissions for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

Permissions for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::<child-account>:role/AppViewX-S3-Bucket-Access"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

AWS IAM Prerequisites for Child Account

Permissions for Establishing a Trust Relationship in Child Accounts

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::master-account-number:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  }
 ]
}
```

Permissions for Discovering and Managing Certificates in IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:UploadServerCertificate",
        "iam:ListServerCertificateTags",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate",
        "ec2:DescribeRegions"
      ],
      "Resource": "*"
    }
  ]
}
```

Permissions for Managing SSM Permissions for the EC2 Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ec2:DescribeInstances",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "s3:ListAllMyBuckets",
  "ssm:DescribeInstanceInformation",
  "ssm:GetDocument",
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
          ],
          "Resource": "*"
      }
   ]
}
```

Permissions for Managing SSM Permissions for EC2 Role

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "ssm:DescribeDocument",
            "ec2messages:GetEndpoint",
            "ec2messages:GetMessages",
            "ssmmessages:OpenControlChannel",
            "ec2messages:DeleteMessage",
            "ssm:UpdateInstanceInformation",
            "ec2messages:FailMessage",
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
         ],
         "Resource": "*",
         "Effect": "Allow"
      },
      {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Onboarding Certificates for AWS Resources in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for AWS Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)
***Select Account View**	**Note:** This field is displayed only when you've selected **Account type** = **Cross account sign-in**. From the given options, select one to specify if the discovery will be performed for the master account or for the child accounts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Select Filter Type**	**Note:** This field is enabled when: • • **Account type** = **Stand-alone account sign-in** • **Account type** = **Cross account sign-in** AND **Select Account View** = **Child Account**. From the following options, select one to specify how the discovery results should be filtered: • **Account View** • **Service View**
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are listed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to AWS Resources with IAM Integration

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for AWS Resources with IAM Integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **AWS**.
Service Types	From the dropdown list, **IAM**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	In this field, enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For AWS, this field is enabled by default and is non-editable.

5. Enter the **Certificate Tags**.
   A certificate tag is a label that you can assign to a certificate. To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

   To enter the certificate tags:

   a. **Enter Key** and **Enter Value**, in the respective fields, for the tag.

   b. Click **Add**.
      The tag, as a key-value pair, is listed in the table shown below the fields.

6. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

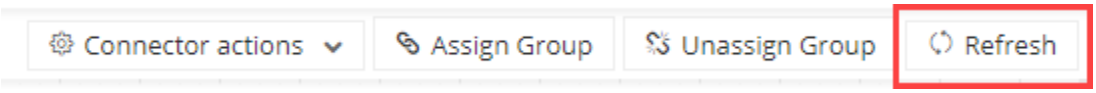
a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.

The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Troubleshooting for AWS IAM

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ACM & IAM service like server addition using AppViewX, fetch, certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Browser	Version	Notes
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Issues in Server Addition using AppViewX GUI

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	Provided credential is invalid.	1. Provide valid Access Key. 2. Provide valid Secret Key.
Provide valid account name	Account name can be duplicate or not as per standard.	1. Provide unique name for account name. 2. Account name can be alphanumeric and can also have period (.) in it.
Details Incorrect	Provide mandatory fields.	Enter mandatory fields like 1. Account Number 2. Access Key 3. Secret Key 4. Data Center

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
		5. Services 6. Regions

Issues in Fetch Regions

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide valid credentials	The provided credential is invalid.	1. Provide valid Access Key. 2. Provide a valid Secret key.

Issues in Discovery in IAM

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or the length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the Discover By section.	Select at least one device from which to discover certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Push and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, such as in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	Userdoes not have required permissions to push to the device.	Retry after getting the access for required action.
Private key content is unavailable.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn’t proceed because push was not successful.	Only successfully pushed certificates can be rolled back.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.

References

- Create an IAM user in your AWS account.
- Create access keys for the root user.
- Create IAM policies using the JSON editor.
- Accessing member accounts.
- Using IAM roles for Amazon EC2 instances.
- Define custom IAM permissions for customer managed policies.

With ELB Integration

This document will guide you through the process of integrating the ELB AWS service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Elastic Load Balancer (ELB)

Elastic Load Balancer, ELB, is a service that automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in one or more Availability Zones. ELB helps ensure the availability, scalability, and fault tolerance of your applications.

AWS provides three types of load balancers:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Application Load Balancer** (**ALB**): Best suited for HTTP and HTTPS traffic, providing advanced request routing features targeted at the delivery of modern application architectures, including microservices and containers.
- **Network Load Balancer** (**NLB**): Designed to handle millions of requests per second while maintaining ultra-low latencies, best suited for TCP, UDP, and TLS traffic where extreme performance is required.
- **Classic Load Balancer** (**CLB**): Provides support for basic load balancing of HTTP/HTTPS and TCP/SSL traffic

Onboarding AWS Resources with ELB Integration in AppViewX

Onboarding AWS Standalone Accounts in AppViewX

A standalone AWS account operates independently with its own set of resources and is not connected to any other AWS accounts.

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important:

- AWS standalone device migration is supported only from the following versions of CERT + SaaS: v2020.1, v2020.2, v2020.3 - v2020.3 FP7. The following prerequisites are also applicable to only these versions.
- AWS device migration is not supported from the following versions of CERT+ SaaS: v2012.x, v2019.x, and v2021.x. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- For customers migrating from versions 20.1.x, 20.2.x, and 20.3.6, AppViewX recommends that you delete the following before migration:
  - All of their Amazon CA settings
  - Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).
- For customers migrating from version v2020.3.10 (mandatory):
  - Delete all of their Amazon CA settings before migration.
  - Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the standalone AWS cloud accounts migrated from the above listed versions to version v2022.1 FP1:

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.

   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.

   The **Device :: Cloud** page is displayed.
3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

   Troubleshooting: If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.
4. From the top-right corner of the **Device :: Coud** page, click the (**Fetch config**).

   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

Note: For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

- Before migration
  1. Merge permissions from all individual buckets into any one S3 bucket.
- After migration
  1. Select a migrated standalone account from the **Device :: Cloud** page.

     The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
  2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
  3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
  4. Click **Add**.
  5. Click **Save**.

     Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

Permissions Required for Onboarding Standalone Accounts

IAM Prerequisites for Discovering and Managing SSL Certificates in ELB

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "elasticloadbalancing:ModifyListener",
            "ec2:DescribeInstances",
            "iam:ListServerCertificates",
            "elasticloadbalancing:DescribeTags",
            "ec2:DescribeRegions",
            "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeListeners",
            "ec2:DescribeAvailabilityZones",
            "acm:GetCertificate",
            "elasticloadbalancing:DescribeTargetHealth",
            "acm:ListCertificates",
            "elasticloadbalancing:DescribeTargetGroups",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "elasticloadbalancing:AddListenerCertificates",
            "elasticloadbalancing:DescribeListenerCertificates"
        ],
        "Resource": "*"
    }
  ]
}
```

Onboarding AWS Standalone Accounts with ELB Integration

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, select **Standalone**.
Account name*	Enter the customer's unique AWS account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Account number*	Enter the customer's AWS account number.
Account Description	Enter a description of the device to be added.
Proxy required	To use a proxy server for communication, select this checkbox.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account).
Access Key ID*	Enter the access key for the customer's AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret Access Key*	Enter the secret key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	From the dropdown list, select **ELB**.
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Service region*	Service regions are regions that are supported by the selected service. From the dropdown list, select the service regions that should be scanned for certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: To be able to fetch and select from the available regions, ensure that the credentials have been provided in the **Credentials** section.
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

Onboarding AWS Cross Accounts in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

This section of the documentation will guide you through the process of onboarding an AWS cross account, for both discovery types, in AppViewX. In AWS, cross-account discovery can be set up in two ways:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Organization-based**: A centralized discovery mechanism that automatically finds and accesses resources across accounts in your AWS Organization using built-in trust and roles
- **IAM Policy-based**: A more flexible discovery mechanism that allows to connect to only the required accounts by manually configuring roles and permissions

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Prerequisites for Onboarding a AWS Cross Account in AppViewX

- Ensure that the following configurations are done on the AWS Management Console:
  - In your AWS master account:
    1. Create an IAM user in the AWS master account.
    2. Generate user identity.
    3. Attach policies to the created user.

       For the AWS IAM permissions to be added for the master account, click here.
  - In your AWS child account:
    1. Create a role in the child account in AWS.
    2. Attach policies to the created role.

       For the AWS IAM permissions to be added for the child account, click here.
    3. Create an EC2 role. This will be used to manage the existing EC2 instance in the AppViewX device inventory.
    4. Attach policies to the EC2 role.

       For the AWS IAM permissions for the EC2 policy, click here.

       For the AWS IAM permissions for the EC2 role, click here.

> **Note:** For detailed instructions, you can access the corresponding AWS documentation using the references given here.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

> **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

- Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Onboarding a Cross Account in AppViewX for Organization-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	To onboard a cross account for organization-based discovery: a. Select **Organization Based Discovery**. The **Organization based Discovery** dialog box is displayed. b. Enter/Select the details required to configure organization-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Policy Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the ELB service component(s) required for the CLM operations.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

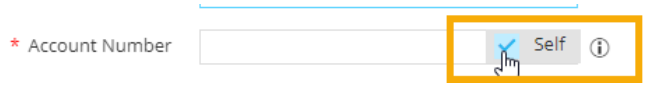
Field	Description
	If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. To add the new device to the cloud device inventory, click **Add**.
9. Click **Save**.
   The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

Note: This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Onboarding a Cross Account in AppViewX for IAM Policy-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	To onboard a cross account for IAM policy-based discovery: a. Select **Policy Based Discovery**. The **Policy based Discovery** dialog box is displayed. b. Enter/Select the details required to configure IAM policy-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Organization Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the ELB service component(s) required for the CLM operations.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. To add the new device to the cloud device inventory, click **Add**.
9. Click **Save**.
   The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.

   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
• In-Progress: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is In-Progress till the resource discovery status for all individual entities is Completed.

Note: This is possible only when the account is in the Managed state.

• Completed: Resource discovery by AppViewX in the customer's AWS environment is complete.

Note: This is possible only when the account is in the Managed state.

Note:
• Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting.
• The resource discovery status of all entities mapped to the account should be Completed.

• Not Applicable: The resource discovery status is set to Not Applicable:
• when Status = Failed or Resolved,
• for ACM and ELB resources,
• for all existing devices and child accounts as part of data migration.
</td></tr>
<tr><td>Cert Discovery Status</td><td>
Note: Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to Not Applicable.

This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values:

• Not started: Certificate discovery for the entity is yet to begin

Note: At this point, the resource discovery status of the associated account can be Not started, In-Progress, or Completed.
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

AWS IAM Prerequisites for Master Account

Permissions for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:GetUserPolicy",
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListAttachedGroupPolicies",
    "iam:ListUserPolicies",
    "iam:GetGroupPolicy",
    "iam:GetUser"
   ],
   "Resource": "*"
  }
 ]
}
```

Permissions for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "organizations:List*"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": [
    "arn:aws:iam::<child account 1>:role/<Assume-role>",
    "arn:aws:iam::<child account 2>:role/< Assume-role>",
    "arn:aws:iam::<child account 3>:role/< Assume-role>"
   ]
  }
 ]
}
```

Permissions for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

Permissions for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::<child-account>:role/AppViewX-S3-Bucket-Access"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

AWS IAM Prerequisites for Child Account

Permissions for Establishing a Trust Relationship in Child Accounts

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::master-account-number:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  }
 ]
}
```

Permissions for Discovering and Managing SSL Certificates in ELB

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GetServerCertificate",
            "elasticloadbalancing:ModifyListener",
            "ec2:DescribeInstances",
            "iam:ListServerCertificates",
            "elasticloadbalancing:DescribeTags",
            "ec2:DescribeRegions",
            "elasticloadbalancing:SetLoadBalancerListenerSSLCertificate",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeListeners",
            "ec2:DescribeAvailabilityZones",
            "acm:GetCertificate",
            "elasticloadbalancing:DescribeTargetHealth",
            "acm:ListCertificates",
            "elasticloadbalancing:DescribeTargetGroups",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "elasticloadbalancing:AddListenerCertificates",
            "elasticloadbalancing:DescribeListenerCertificates"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions for Managing SSM Permissions for the EC2 Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
    "ssm:DescribeDocument",
    "ec2:DescribeInstances",
    "s3:ListAllMyBuckets",
    "ssm:DescribeInstanceInformation",
    "ssm:GetDocument",
    "ssm:CreateDocument",
    "ssm:GetCommandInvocation",
    "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions for Managing SSM Permissions for EC2 Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeDocument",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "ec2messages:GetEndpoint",
            "ec2messages:GetMessages",
            "ssmmessages:OpenControlChannel",
            "ec2messages:DeleteMessage",
            "ssm:UpdateInstanceInformation",
            "ec2messages:FailMessage",
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Onboarding Certificates for AWS Resources in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Discovering Certificates for AWS Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter the details for **initiating a scheduled cloud certificate discovery scan**.

   Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Note: Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)
***Select Account View**	**Note:** This field is displayed only when you've selected **Account type** = **Cross account sign-in**. From the given options, select one to specify if the discovery will be performed for the master account or for the child accounts.
***Select Filter Type**	**Note:** This field is enabled when: • • **Account type** = **Stand-alone account sign-in** • **Account type** = **Cross account sign-in** AND **Select Account View** = **Child Account**. From the following options, select one to specify how the discovery results should be filtered: • **Account View** • **Service View**
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.

5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are listed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to AWS Resources with ELB Integration

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for AWS Resources with ELB Integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **AWS**.
Service Types	From the dropdown list, **ELB**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Certificates can be stored in either AWS Certificate Manager (**ACM**) or AWS Identity and Access Management (**IAM**).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the options given, select the required certificate location.
Certificate ARN	**Note:** This field is displayed when **Certificate Location** = **ACM**. The ARN (Amazon Resource Name) is a unique identifier assigned to each certificate that is managed by ACM. It is used to reference the certificate in API calls, policies, and so on. In this field, enter the ARN of the certificate to be pushed.
***Certificate File Name**	**Note:** This field is displayed when **Certificate Location** = **IAM**. In this field, enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For AWS, this field is enabled by default and is non-editable.
Default Certificate	In the event that a certificate cannot be pushed, a default certificate is pushed as a fall back option. To enable this, select the **Default Certificate** checkbox.

5. Enter the **Certificate Tags**.
   A certificate tag is a label that you can assign to a certificate. To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

   To enter the certificate tags:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. **Enter Key** and **Enter Value**, in the respective fields, for the tag.

b. Click **Add**.

The tag, as a key-value pair, is listed in the table shown below the fields.

6. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.
Post - Push Script File Name	Enter the file name of the post push script.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.

The connector is displayed on the certificate holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

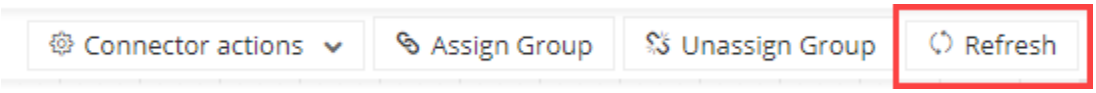
   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting AWS ELB

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for ELB service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post-AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Supported Devices

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Discovery in ELB

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Please provide information as required	1. Discovery name is not given or length is less than 2 characters. 2. Interval between batches info. is missing when execution type is sequential.	1. Enter a valid name with a minimum of 2 characters. 2. Provide a time interval between batches in minutes.
Please select a device	No device is selected in the “Discover By” section.	Select at least one device to discover certificates from.

Issues in Push-Bind and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in progress and not completed. 3. AppConnector might not be in sync.	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.
Unable to initiate request, template is in disabled state	Given workflow is not in an enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
1 validation error detected: Value at 'privateKey' failed to satisfy constraint.	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because the push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to the device when certificate is unavailable, i.e, in a new state.	Push to the device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	The provided certificate is not a valid certificate.	Push a valid certificate.
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide Modify access for the resource and retry
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

- Create an IAM user in your AWS account.
- Create access keys for the root user.
- Create IAM policies using the JSON editor.
- Accessing member accounts.
- Using IAM roles for Amazon EC2 instances.
- Define custom IAM permissions for customer managed policies.

With CloudFront Integration

This document will guide you through the process of integrating the CloudFront AWS service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

CloudFront

CloudFront is a Content Delivery Network (CDN) service. It speeds up the delivery of your web content by caching copies of your content at edge locations around the world.

Onboarding AWS Resources with CloudFront Integration in AppViewX

Onboarding AWS Standalone Accounts in AppViewX

A standalone AWS account operates independently with its own set of resources and is not connected to any other AWS accounts.

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important:

- AWS standalone device migration is supported only from the following versions of CERT + SaaS: v2020.1, v2020.2, v2020.3 - v2020.3 FP7. The following prerequisites are also applicable to only these versions.
- AWS device migration is not supported from the following versions of CERT+ SaaS: v2012.x, v2019.x, and v2021.x. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

- For customers migrating from versions 20.1.x, 20.2.x, and 20.3.6, AppViewX recommends that you delete the following before migration:
  - All of their Amazon CA settings
  - Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).
- For customers migrating from version v2020.3.10 (mandatory):
  - Delete all of their Amazon CA settings before migration.
  - Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the standalone AWS cloud accounts migrated from the above listed versions to version v2022.1 FP1:

For standalone accounts where one of the associated services is not EC2

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.

   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.

   The **Device :: Cloud** page is displayed.
3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

   Troubleshooting: If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.
4. From the top-right corner of the **Device :: Coud** page, click the (**Fetch config**).

   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

Note: For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

- Before migration
  1. Merge permissions from all individual buckets into any one S3 bucket.
- After migration
  1. Select a migrated standalone account from the **Device :: Cloud** page.

     The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.
  2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
  3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
  4. Click **Add**.
  5. Click **Save**.

     Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

Permissions Required for Onboarding Standalone Accounts

IAM Prerequisites for Discovering and Managing SSL Certificates in CloudFront

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "iam:GetServerCertificate",
            "acm:GetCertificate",
            "acm:ListCertificates",
            "iam:ListServerCertificates",
            "ec2:DescribeRegions",
            "cloudfront:ListDistributions",
            "acm:ImportCertificate",
            "acm:AddTagsToCertificate",
            "acm:ListTagsForCertificate",
            "acm:RemoveTagsFromCertificate",
            "cloudfront:UpdateDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListTagsForResource",
            "iam:UploadServerCertificate",
            "iam:ListServerCertificateTags",
            "iam:TagServerCertificate",
            "iam:UntagServerCertificate"
        ],
        "Resource": "*"
    }
  ]
}
```

Onboarding AWS Standalone Accounts with CloudFront Integration

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, select **Standalone**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account name*	Enter the customer's unique AWS account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Account number*	Enter the customer's AWS account number.
Account Description	Enter a description of the device to be added.
Proxy required	To use a proxy server for communication, select this checkbox.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account).
Access Key ID*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret Access Key*	Enter the secret key for the customer's AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when **Credential** type is set to **Manual Entry**.
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	From the dropdown list, select **CloudFront**.
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Custom SSL Client Support	For configuring custom SSL client support for CloudFront, from the dropdown list, you need to specify how CloudFront will handle the SSL/TLS connections from different types of clients.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select one from the following options: • **Clients that Support Server Name Indication** Server Name Indication (SNI) is an extension of the SSL/TLS protocol that allows a client to specify the hostname it is trying to connect to at the start of the handshake process. This allows a server to present multiple SSL/TLS certificates on the same IP address and TCP port number, enabling the use of different certificates for different domains. • **Legacy Clients Support'** **Legacy clients** refer to older browsers and devices that do not support SNI. These clients cannot specify the hostname during the SSL/TLS handshake, meaning they may not be able to establish a secure connection if the server relies on SNI to serve the correct certificate.
Security Policy	The security policy determines which cryptographic algorithms and protocols are available for secure communication, ensuring data integrity, confidentiality, and protection against various security threats. From the dropdown list, select the protocol CloudFront will use to establish secure SSL/TLS connections with viewers.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

Onboarding AWS Cross Accounts in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

This section of the documentation will guide you through the process of onboarding an AWS cross account, for both discovery types, in AppViewX. In AWS, cross-account discovery can be set up in two ways:

- **Organization-based**: A centralized discovery mechanism that automatically finds and accesses resources across accounts in your AWS Organization using built-in trust and roles
- **IAM Policy-based**: A more flexible discovery mechanism that allows to connect to only the required accounts by manually configuring roles and permissions

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Prerequisites for Onboarding a AWS Cross Account in AppViewX

- Ensure that the following configurations are done on the AWS Management Console:
  - In your AWS master account:
    1. Create an IAM user in the AWS master account.
    2. Generate user identity.
    3. Attach policies to the created user.

       For the AWS IAM permissions to be added for the master account, click here.
  - In your AWS child account:
    1. Create a role in the child account in AWS.
    2. Attach policies to the created role.

       For the AWS IAM permissions to be added for the child account, click here.
    3. Create an EC2 role. This will be used to manage the existing EC2 instance in the AppViewX device inventory.
    4. Attach policies to the EC2 role.

       For the AWS IAM permissions for the EC2 policy, click here.

       For the AWS IAM permissions for the EC2 role, click here.

> **Note:** For detailed instructions, you can access the corresponding AWS documentation using the references given here.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

> **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

- Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Onboarding a Cross Account in AppViewX for Organization-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	To onboard a cross account for organization-based discovery: a. Select **Organization Based Discovery**. The **Organization based Discovery** dialog box is displayed. b. Enter/Select the details required to configure organization-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Policy Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the CloudFront service component required for the CLM operations.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

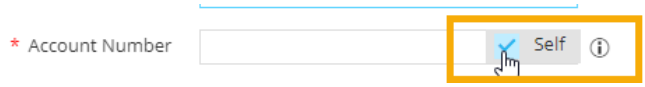
Field	Description
	If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. To add the new device to the cloud device inventory, click **Add**.
9. Click **Save**.
   The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section. To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

Note: This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Onboarding a Cross Account in AppViewX for IAM Policy-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	To onboard a cross account for IAM policy-based discovery: a. Select **Policy Based Discovery**. The **Policy based Discovery** dialog box is displayed. b. Enter/Select the details required to configure IAM policy-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Organization Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the CloudFront service component required for the CLM operations.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. To add the new device to the cloud device inventory, click **Add**.
9. Click **Save**.
   The added device is listed in the outer inventory on the **Device :: Cloud** page.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.

   The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device

Status	Status of the discovered accounts.
	
	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state. **Note:** • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**. **Note:** Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

AWS IAM Prerequisites for Master Account

Permissions for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:GetUserPolicy",
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListAttachedGroupPolicies",
    "iam:ListUserPolicies",
    "iam:GetGroupPolicy",
    "iam:GetUser"
   ],
   "Resource": "*"
  }
 ]
}
```

Permissions for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "organizations:List*"
        ],
        "Resource": "*"
    }
  ]
}
```

Permissions for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": [
    "arn:aws:iam::<child account 1>:role/<Assume-role>",
    "arn:aws:iam::<child account 2>:role/< Assume-role>",
    "arn:aws:iam::<child account 3>:role/< Assume-role>"
   ]
  }
 ]
}
```

Permissions for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

Permissions for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::<child-account>:role/AppViewX-S3-Bucket-Access"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

AWS IAM Prerequisites for Child Account

Permissions for Establishing a Trust Relationship in Child Accounts

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::master-account-number:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    }
  ]
}
```

Permissions for Discovering and Managing SSL Certificates in CloudFront

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:GetServerCertificate",
                "acm:GetCertificate",
                "acm:ListCertificates",
                "iam:ListServerCertificates",
                "ec2:DescribeRegions",
                "cloudfront:ListDistributions",
                "acm:ImportCertificate",
                "acm:AddTagsToCertificate",
                "acm:ListTagsForCertificate",
                "acm:RemoveTagsFromCertificate",
                "cloudfront:UpdateDistribution",
                "cloudfront:GetDistributionConfig",
                "cloudfront:ListTagsForResource",
                "iam:UploadServerCertificate",
                "iam:ListServerCertificateTags",
                "iam:TagServerCertificate",
                "iam:UntagServerCertificate"
            ],
            "Resource": "*"
        }
    ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Managing SSM Permissions for the EC2 Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
    "ssm:DescribeDocument",
    "ec2:DescribeInstances",
    "s3:ListAllMyBuckets",
    "ssm:DescribeInstanceInformation",
    "ssm:GetDocument",
    "ssm:CreateDocument",
    "ssm:GetCommandInvocation",
    "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions for Managing SSM Permissions for EC2 Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeDocument",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ssmmessages:OpenControlChannel",
                "ec2messages:DeleteMessage",
                "ssm:UpdateInstanceInformation",
                "ec2messages:FailMessage",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Onboarding Certificates for AWS Resources in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for AWS Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	• **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)
***Select Account View**	**Note:** This field is displayed only when you've selected **Account type** = **Cross account sign-in**. From the given options, select one to specify if the discovery will be performed for the master account or for the child accounts.
***Select Filter Type**	**Note:** This field is enabled when: • • **Account type** = **Stand-alone account sign-in** • **Account type** = **Cross account sign-in** AND **Select Account View** = **Child Account**. From the following options, select one to specify how the discovery results should be filtered: • **Account View** • **Service View**
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are listed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to AWS Resources with CloudFront Integration

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for AWS Resources with CloudFront Integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **AWS**.
Service Types	From the dropdown list, **CloudFront**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Certificates can be stored in either AWS Certificate Manager (**ACM**) or AWS Identity and Access Management (**IAM**).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the options given, select the required certificate location.
Certificate ARN	**Note:** This field is displayed when **Certificate Location** = **ACM**. The ARN (Amazon Resource Name) is a unique identifier assigned to each certificate that is managed by ACM. It is used to reference the certificate in API calls, policies, and so on. In this field, enter the ARN of the certificate to be pushed.
***Certificate File Name**	**Note:** This field is displayed when **Certificate Location** = **IAM**. In this field, enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For AWS, this field is enabled by default and is non-editable.

5. Enter the **Certificate Tags**.
   A certificate tag is a label that you can assign to a certificate. To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

   To enter the certificate tags:

   a. **Enter Key** and **Enter Value**, in the respective fields, for the tag.

   b. Click **Add**.
      The tag, as a key-value pair, is listed in the table shown below the fields.

6. Enter/Select the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.
Post - Push Script File Name	Enter the file name of the post push script.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

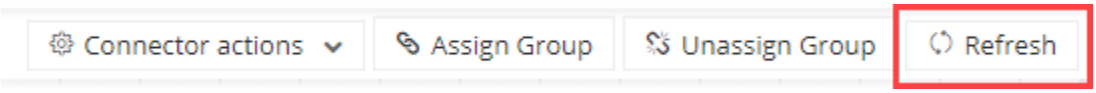
   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting AWS CloudFront

Overview

This section helps you troubleshoot the common problems that you might encounter when using AWS cloud functionalities for CloudFront service. This guide will give more troubleshooting processes on certificate discovery & certificate push.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	NA
Chrome	Till latest (Version 80.0)	NA
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Issues in Discovery in CloudFront

Issues in Push-Bind and Rollback

Error messages and resolutions

Error Message	Possible Cause	Possible Solution
Unable to initiate request.	1. Pushing to device when certificate is unavailable, i.e, in a new state. 2. Previous work order is in	1. Push to device after certificate has been retrieved from CA. 2. Initiate push after previous work order is finished. 3. Synchronize the AppConnector and retry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
	progress and not completed. 3. AppConnector might not be in sync.	
Unable to initiate request, template is in disabled state	Given workflow is not in enabled state	Enable the push/rollback workflow from the Workflow section.
User is not authorized	User does not have required permissions to push to the device.	Retry after getting the access for required action.
Private Key is required to push certificate to ACM inventory	Private key content is not available for the certificate.	Private key is mandatory for the certificate to be pushed.
Application connector(s) not found	Application connector info was not found.	Provide the correct connectorId if not pushing using AppViewX UI.
Request associated with the application connector is in progress	Previous work order is in progress and not completed.	Initiate this request after the previous work order is finished.
Push not triggered or succeeded or No existing data available for backup process.	Rollback couldn't proceed because push was not successful.	Only successfully pushed certificates can be rolled back.
Certificate not found.	Pushing to device when certificate is unavailable, i.e, in a new state.	Push to device after certificate has been retrieved from CA.
Provided certificate is not a valid self signed. Please provide either a valid self-signed certificate or certificate chain	Provided certificate is not a valid certificate.	Push a valid certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error messages and resolutions (continued)

Error Message	Possible Cause	Possible Solution
Push failed as there exists another certificate with commonName	Certificate with the same common name is present in certificate manager	Check whether it is a duplicate certificate and remove the invalid one.
Cert Association failed with profile	Modify access may not be available on the selected resource	Provide “Modify” access for the resource and retry.
Association failed with profile-<PROFILE_NAME>as no such profile available	Profile may not be available on the cloud account	Perform config fetch on the device from ADC module and retry association of cert.
Certificate cannot be pushed as selected Amazon CA certificate is in <SOURCE_REGION> region and region you tried is <DESTINATION_REGION>	Selected certificate is in ACM in a different region than the region to be pushed	Use certificates available in the <DESTINATION_REGION> (or) Push a new certificate to the <DESTINATION_REGION>

References

- Create an IAM user in your AWS account.
- Create access keys for the root user.
- Create IAM policies using the JSON editor.
- Accessing member accounts.
- Using IAM roles for Amazon EC2 instances.
- Define custom IAM permissions for customer managed policies.

With EC2 Integration

This document will guide you through the process of integrating the EC2 AWS service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2) is a web service provided by Amazon Web Services (AWS) that offers resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers by providing a secure, resizable, and flexible environment for running applications.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding AWS Resources with EC2 Integration in AppViewX

Onboarding AWS Standalone Accounts in AppViewX

A standalone AWS account operates independently with its own set of resources and is not connected to any other AWS accounts.

Prerequisites for Migrating AWS Standalone Accounts from Older Versions

Important:

- AWS standalone device migration is supported only from the following versions of CERT + SaaS: v2020.1, v2020.2, v2020.3 - v2020.3 FP7. The following prerequisites are also applicable to only these versions.
- AWS device migration is not supported from the following versions of CERT+ SaaS: v2012.x, v2019.x, and v2021.x. For these versions, it is recommended that you delete all AWS devices (both, standalone and cross accounts) before migration and add them after the migration to 22.1 is complete.

Note:

- For customers migrating from versions 20.1.x, 20.2.x, and 20.3.6, AppViewX recommends that you delete the following before migration:
  - All of their Amazon CA settings
  - Any EC2 instances that were added manually from the server inventory (excluding the EC2 instances auto-discovered from the cloud accounts).
- For customers migrating from version v2020.3.10 (mandatory):
  - Delete all of their Amazon CA settings before migration.
  - Trigger config fetch for all of their cloud accounts after migration.

The following actions have to be performed for the standalone AWS cloud accounts migrated from the above listed versions to version v2022.1 FP1:

For standalone accounts where one of the associated services is not EC2

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. After you have upgraded the product from a version < v2020.3 FP8 to v2022.1 FP1, from the top left corner of the AppViewX user interface, go to (**Menu**) > **CERT+** > **Administration** > **Device Management**.

   The **Device :: ADC** page is displayed.

2. From the **Device :: ADC** page, select **Cloud**.

   The **Device :: Cloud** page is displayed.

3. From the device accounts listed under **Account Name**, select the required migrated standalone accounts.

   Troubleshooting: If you cannot see the migrated standalone accounts listed, request the super user to grant you the required permissions. Only **superusers** and users authorized by the superuser can view these migrated accounts in the list.

4. From the top-right corner of the **Device :: Coud** page, click the (**Fetch config**).

   This step is mandatory to upgrade the data recorded for the older devices to the latest format followed in v2022.1 FP1.

For standalone accounts where one of the associated services is EC2

In versions v2020.1/v2020.2/v2020.3-v2020.3FP7, for accounts in which multiple regions are associated with the EC2 service, individual S3 buckets are used to store the permissions for each region.

In v2022.1 FP1, this has been modified to use only one S3 bucket to store the permissions for all regions, irrespective of the number of associated regions.

Note: For accounts with only one associated service region, skip the following steps, since only one S3 bucket includes all permissions anyway. For such accounts, trigger **Fetch Config** manually from the inventory page.

- Before migration
  1. Merge permissions from all individual buckets into any one S3 bucket.
- After migration
  1. Select a migrated standalone account from the **Device :: Cloud** page.

     The **Device :: Cloud > Modify** page is displayed, with the details of the selected account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. In the **Amazon Cloud Service Settings** section, click **Fetch collection type**.
3. From the **Collection type** dropdown list, select the S3 bucket into which all permissions for this account were merged.
4. Click **Add**.
5. Click **Save**.

   Fetch Config is automatically triggered and the account details are upgraded according to the latest version.

Permissions Required for Onboarding Standalone Accounts

IAM Prerequisites for Managing SSM Permissions for the EC2 Policy

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "ssm:SendCommand",
  "ssm:DescribeDocument",
  "ec2:DescribeInstances",
  "s3:ListAllMyBuckets",
  "ssm:DescribeInstanceInformation",
  "ssm:GetDocument",
  "ssm:CreateDocument",
  "ssm:GetCommandInvocation",
  "ec2:DescribeRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

IAM Prerequisites for Managing SSM Permissions for EC2 Role

```
{
   "Version": "2012-10-17",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  "Statement": [
    {
      "Action": [
        "ssm:DescribeDocument",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ssmmessages:OpenControlChannel",
        "ec2messages:DeleteMessage",
        "ssm:UpdateInstanceInformation",
        "ec2messages:FailMessage",
        "ssmmessages:OpenDataChannel",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ec2messages:AcknowledgeMessage",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ec2messages:SendReply"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject",
        "s3:GetEncryptionConfiguration",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::appviewx-s3/*",
        "arn:aws:s3:::appviewx-s3"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

IAM Prerequisites for Enabling S3 Bucket Access to AppViewX

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
  "s3:ListBucket",
  "s3:DeleteObject",
  "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::appviewx-s3/*",
        "arn:aws:s3:::appviewx-s3"
      ],
    }
  ]
}
```

Onboarding AWS Standalone Accounts with EC2 Integration

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Account Type*	From the dropdown list, select **Standalone**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Account name*	Enter the customer's unique AWS account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Account number*	Enter the customer's AWS account number.
Account Description	Enter a description of the device to be added.
Proxy required	To use a proxy server for communication, select this checkbox.
Data center*	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
Credential type*	From the dropdown list, from the following options, select the credential type: • **Manual Entry**: Manually enter the access and secret key for the customer's AWS account).
Access Key ID*	Enter the access key for the customer's AWS account. **Note:** This field is displayed only when **Credential** type is set to **Manual Entry**.
Secret Access Key*	Enter the secret key for the customer's AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field is displayed only when **Credential** type is set to **Manual Entry**.
Credential name*	If the customer's AWS credentials are stored in CyberArk, from the dropdown list, select the CyberArk credential name. **Note:** This field is displayed only when **Credential** type is set to **Credential List - CyberArk**.
**: Mandatory Fields*	

7. Enter/Select the details for the **Amazon Cloud Service Settings**.

Field description for the Amazon Cloud Service Settings section

Field	Description
Services*	From the dropdown list, select **EC2**.
Default region*	Based on the customer's requirement, select the default region in which the customer's AWS cloud account is deployed. AppViewX will use this region to communicate with the other (geographically farther) regions.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Cert sync	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
**: Mandatory Fields*	

8. Click **Add**.
   Account details are now available in the device inventory. Once the account is onboarded, you can discover the corresponding certificates and manage them.

Onboarding AWS Cross Accounts in AppViewX

AppViewX streamlines the management and visibility of your AWS resources by putting in place a simple workflow that lets you onboard your AWS resources onto AppViewX's holistic certificate lifecycle management solution. One part of this configuration will be done on the AWS management console and the rest of the configuration will be facilitated via the AppViewX interface.

You can onboard the following AWS account types to AppViewX: a standalone account (all resources are available in the same account) and a cross or federated account (resources are distributed across multiple accounts).

This section of the documentation will guide you through the process of onboarding an AWS cross account, for both discovery types, in AppViewX. In AWS, cross-account discovery can be set up in two ways:

- **Organization-based**: A centralized discovery mechanism that automatically finds and accesses resources across accounts in your AWS Organization using built-in trust and roles
- **IAM Policy-based**: A more flexible discovery mechanism that allows to connect to only the required accounts by manually configuring roles and permissions

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: The following steps cover only the bare minimum requirements for onboarding a cross account AWS account in AppViewX. The optional fields are out of scope and their configuration is left to the discretion of the user.

Prerequisites for Onboarding a AWS Cross Account in AppViewX

- Ensure that the following configurations are done on the AWS Management Console:
  - In your AWS master account:
    1. Create an IAM user in the AWS master account.
    2. Generate user identity.
    3. Attach policies to the created user.

       For the AWS IAM permissions to be added for the master account, click here.
  - In your AWS child account:
    1. Create a role in the child account in AWS.
    2. Attach policies to the created role.

       For the AWS IAM permissions to be added for the child account, click here.
    3. Create an EC2 role. This will be used to manage the existing EC2 instance in the AppViewX device inventory.
    4. Attach policies to the EC2 role.

       For the AWS IAM permissions for the EC2 policy, click here.

       For the AWS IAM permissions for the EC2 role, click here.
  - If account specific S3 buckets have been deployed for EC2 integration, ensure that the bucket names are suffixed with the corresponding account number.

    For instruction on creating an S3 bucket in your AWS account, see References.

> **Note:** For detailed instructions, you can access the corresponding AWS documentation using the references given here.

- If credentials for onboarding have to be fetched from a credential list in CyberArk:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Ensure that your AWS access credentials are saved in your CyberArk account. For instructions on creating AWS access details in the CyberArk account , refer to the documentation here.

> **Important:** For this use case, in the Account Parameters, the **Password** field must be considered a mandatory parameter. This field is used to specify the AWS access secret key information.

- Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.

Onboarding a Cross Account in AppViewX for Organization-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Discovery Mode*	To onboard a cross account for organization-based discovery: a. Select **Organization Based Discovery**. The **Organization based Discovery** dialog box is displayed. b. Enter/Select the details required to configure organization-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Policy Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the EC2 service component(s) required for the CLM operations. For the EC2 service, a set of additional fields is displayed, the instructions for which are covered in the subsequent steps.
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **EC2 Services** section.

Field description for the EC2 Services section

Field	Description
Communication mode	By default, the **SSM** communication mode is selected.
Certificate Discovery Mode	By default, the **File System Scanning** certificate discovery mode is selected.
***S3 Deployment Type**	From the dropdown list, from the following options, select the deployment type used for the S3 bucket that will be used for the EC2 integration: • **Centralized**: Select this if the S3 bucket that will be used for the EC2 integration is managed centrally across all accounts. • **Account Specific**: Select this if each account manages individual S3 buckets.
***S3 Bucket Name**	Enter the name of the S3 bucket that will be used for EC2 integration. For account specific S3 buckets, enter the bucket name **without** the account number suffix. AppViewX will automatically append the account number based on the value entered here. To configure the ARN advanced settings for the specified S3 bucket, follow the instructions given below: a. Click . The **ARN Advanced Settings** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>b. In the ARN Advanced Settings dialog box, enter the following details:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Role ARN*</td><td>Amazon Resource Name of the role that the caller is assuming.</td></tr>
<tr><td>Role Session name*</td><td>Role Session name is an identifier for the assumed role session.

Use the Role Session name to uniquely identify a session when the same rule is assumed by different principals or for different reasons.</td></tr>
<tr><td>Duration Seconds</td><td>Enter the duration, in seconds, for which the credentials should remain valid.

Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
• Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

9. To add the new device to the cloud device inventory, click **Add**.
10. Click **Save**.

    The added device is listed in the outer inventory on the **Device :: Cloud** page.

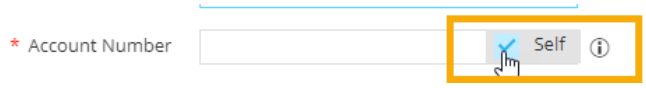
Configuring Organization Based Discovery

1. In the **Organization based discovery** popup window, under **Organisation Accounts**, enter/select the discovery details.

Field description for the Organisation Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Account Number*	By default, the AWS account number is automatically fetched from the value entered in the Account Number field in the Basic information section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To enter a different account number: a. From the **Account Number** field in the **Organization based discovery popup** window, click **Self**.  b. Enter the required account number.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

2. Enter/Select the required details in the **Child Accounts** section.

Field description for the Child Accounts section

Field	Description
Role Name*	Enter the IAM role name for the target account here.
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

3. Click **Save**.
   The **Organization based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

> **Note:**
> - If the popup is closed without values entered for at least one field, then the **Organization based discovery** checkbox will be unchecked.
> - Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **Organization based discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
*: Mandatory fields	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Onboarding a Cross Account in AppViewX for IAM Policy-based Discovery

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On to the **Device :: Cloud** page and click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of Vendors, select **AWS**.
5. Enter/Select the **Basic information**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Basic Information section

Field	Description
***Account Type**	From the dropdown list, from the following options, select **Cross or Federated**.
***Account name**	Enter your AWS account name. **Constraints**: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Account number**	Enter your AWS account number.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credentials**-related information.

Field description for the Credentials section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating AWS with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **IAM ROLE ACCESS** Tech Preview: An IAM role-based approach is used for authentication instead of direct access keys. **Important:** This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production.
***Access key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the access key generated for your AWS account.
***Secret key**	This field is displayed when **Credential type** = **Manual Entry**. Enter the secret key generated for your AWS account.
Download Cloud Formation Template (CFT)	This clickable link is displayed when **Credential type** = **IAM ROLE ACCESS**. To download the CloudFormation template, click this link. The downloaded CFT is pre-configured with all account details and permissions that have to be assigned to the IAM role and can be directly deployed in your AWS environment. To read more on CloudFormation templates, read the documentation here.
***Master Account Role**	Enter the Amazon Resource Name (ARN) of the AWS IAM role.
***External Id**	Enter the unique identifier generated to establish a secure trust relationship between AWS and AppViewX.
***Credential List**	This field is displayed when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the AWS credentials that will be used for onboarding the standalone account.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the information required to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
Auto Discover Resources	To discover all the cross or federated/child accounts for the master account details provided, enable this field.
Advanced Settings	To customize the auto discovery process, enable this field.
Auto Discovery Mode*	To onboard a cross account for IAM policy-based discovery: a. Select **Policy Based Discovery**. The **Policy based Discovery** dialog box is displayed. b. Enter/Select the details required to configure IAM policy-based discovery. **Note:** For the Auto Discovery Mode, you can select both options, Organization Based Discovery as well as Policy Based Discovery. For instructions on configuring Organization Based Discovery, click here.
Service*	From the **Select the Service(s)** dropdown list, select the EC2 service component(s) required for the CLM operations. For the EC2 service, a set of additional fields is displayed, the instructions for which are covered in the subsequent steps.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Service Region*	To select a service region: a. To fetch the service regions for the account information provided, click **Fetch Region.** The retrieved service regions are populated in the **Select the Region(s)** dropdown list. b. From the **Select the Region(s)** dropdown list, select the required service region.
Cert Sync*	Select from one of the following options: • **Managed**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's AWS account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's AWS account but certificate discovery will be disabled.
Auto Sync	To enable/disable automatic synchronization, use the **Auto Sync** key. If **Auto Sync** is enabled, select the checkbox for the type of synchronization from the following options: • **Trigger Based** (For steps on configuring trigger-based sync, click here.) • **Schedule Based** (For steps on configuring schedule-based sync, click here.)
**: Mandatory fields*	

8. Enter/Select the required details in the **EC2 Services** section.

Field description for the EC2 Services section

Field	Description
Communication mode	By default, the **SSM** communication mode is selected.
Certificate Discovery Mode	By default, the **File System Scanning** certificate discovery mode is selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***S3 Deployment Type**	From the dropdown list, from the following options, select the deployment type used for the S3 bucket that will be used for the EC2 integration: • **Centralized**: Select this if the S3 bucket that will be used for the EC2 integration is managed centrally across all accounts. • **Account Specific**: Select this if each account manages individual S3 buckets.
***S3 Bucket Name**	Enter the name of the S3 bucket that will be used for EC2 integration. For account specific S3 buckets, enter the bucket name **without** the account number suffix. AppViewX will automatically append the account number based on the value entered here. To configure the ARN advanced settings for the specified S3 bucket, follow the instructions given below: a. Click . The **ARN Advanced Settings** dialog box is displayed. b. In the **ARN Advanced Settings** dialog box, enter the following details: **Field** / **Description** **Role ARN*** — Amazon Resource Name of the role that the caller is assuming. **Role Session name*** — **Role Session name** is an identifier for the assumed role session. Use the **Role Session name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons. **Duration Seconds** — Enter the duration, in seconds, for which the credentials should remain valid.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>Acceptable durations for IAM user sessions:
• Minimum: 900 seconds (15 minutes)
• Maximum: 129,600 seconds (36 hours)
• Default: 3600 seconds (1 hour)</td></tr>
<tr><td>External Id</td><td>External Id is a unique identifier that might be required when you assume a role in another account.</td></tr>
<tr><td>Source Identity</td><td>The source identity is specified by the principal that is calling the AssumeRole operation.</td></tr>
<tr><td>Session Tags</td><td>Session Tags are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS.

To create a session tag:
i. In the Enter Key field, enter a key for the key-value pair.
ii. In the Enter Value field, enter a value for the key-value pair.
iii. Click Add.

The added key-value pair is shown in the table below the fields.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

9. To add the new device to the cloud device inventory, click **Add**.
10. Click **Save**.

    The added device is listed in the outer inventory on the **Device :: Cloud** page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Configuring IAM Policy Based Discovery

1. In the **IAM Policy based discovery** popup window enter/select the **Child Accounts** details.

Field description for the Child Accounts section

Field	Description
Role Session Name	**Role Session Name** is an identifier for the assumed role session. Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.

2. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The **IAM Policy based discovery** popup window is closed and you will be navigated back to the **Discover resources** section.

Note:

- If the popup is closed without values entered for at least one field, then the**IAM Policy based discovery** checkbox will be unchecked.
- Values once saved in the popup will be stored and made available on the screen always, regardless of the number of times the **IAM Policy Based Discovery** checkbox is checked or unchecked, unless the values are updated.

Configuring Trigger Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Trigger Based**.
   The **Trigger Based Sync** popup window is displayed.
2. Enter/Select the required **Queue Parameter** details.

Field description for the Queue Parameter section

Field	Description
SQS URL*	Enter the URL of the SQS queue.
Dead Letter Queue	Enter the URL of the Dead Letter Queue. **Note:** This field is optional and can be used for user reference purposes only. Currently, AppViewX does not have any insights based on DLQ messages.
**: Mandatory fields*	

3. Enter/Select the **STS Token** details.

Field description for the STS Token section

Field	Description
Role ARN*	Enter the Amazon Resource Name that will interact with the SQS queue through the AWS STS.
Role Session name	**Role Session Name** is an identifier for the assumed role session.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Use the **Role Session Name** to uniquely identify a session when the same rule is assumed by different principals or for different reasons.
Duration Seconds	Enter the duration, in seconds, for which the credentials should remain valid. Acceptable durations for IAM user sessions: • **Minimum**: 900 seconds (15 minutes) • **Maximum**: 129,600 seconds (36 hours) • **Default**: 3600 seconds (1 hour)
External Id	**External Id** is a unique identifier that might be required when you assume a role in another account.
Source Identity	The source identity is specified by the principal that is calling the **AssumeRole** operation.
Session Tags	**Session Tags** are key-value pairs that you pass when you assume an IAM role or federate a user in AWS STS. To create a session tag: a. In the **Enter Key** field, enter a key for the key-value pair. b. In the **Enter Value** field, enter a value for the key-value pair. c. Click **Add**. The added key-value pair is shown in the table below the fields.
**: Mandatory fields*	

4. Enter/Select the **SQS Attributes**.

Field description for the SQS Attributes section

Field	Description
SQS Polling Interval*	Enter an interval value for the SQS message polling from AppViewX.
Max Number of Messages*	Enter the maximum number of messages that will be returned by the queue per request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Visibility Timeout in Minutes*	After messages are retrieved by a **ReceiveMessage** request, they need to be made invisible to subsequent retrieve requests for a custom duration. In this field, enter this duration in minutes.
Wait time in seconds*	Enter a duration, in seconds, for which a call will wait for a message to arrive in the queue before returning.
**: Mandatory fields*	

5. In the **Auto Sync Services** section, select the list of services for which the trigger-based sync mechanism is required.
6. In the **Service Specific Parameters** section, from the **EC2 Sync Delay Time** dropdown list, select the delay interval (in hours) for the synchronization of EC2 instances when they are discovered for the first time.

> **Note:** This section is displayed only if the EC2 service is selected in the **Auto Sync Services** section.

7. Click **Apply**.

Configuring Schedule Based Sync

1. In the **Discover Resources** section, enable **Auto Sync** and select **Schedule Based**.
   The **Schedule Based Sync** popup window is displayed.
2. Enter/Select the **General Information**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the General Information section

Field	Description
Frequency of Sync*	To schedule the sync, set a frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	For the current release, this field is set to **Off** and is disabled. This field and the associated features will be enabled in the upcoming release.
**: Mandatory fields*	

3. Click **Apply**.

Account Level/Inner Inventory

For the child accounts added, this table explains the fields that AppViewX displays to show the details of each account.

Field	Description
Account Name	Name of the account to which the cloud device belongs
Role Name	Role name of the account creator
Service Region	The service region selected for the account
Service	Service integrated for the cloud device
Status	Status of the discovered accounts.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	This field takes the following values:
	
	• For the master account:
	  • **Managed**
	  • **Failed**
	• For the child account:
	  • **Success**
	  • **Partial Success**
	  • **Queued**
	  • **In Progress**
	  • **Failed**

Resource Discovery Status	**Note:** Resource discovery status is not applicable for master accounts. For master accounts, the resource discovery status is set to **Not Applicable**. This field indicates the status of the resource discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Resource discovery for the entity is yet to begin. **Note:** At this point, it is not mandatory for the associated account to be in the **Managed** (account credentials validated) state. • **In-Progress**: Resource discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The aggregated resource discovery status is **In-Progress** till the resource discovery status for all individual entities is **Completed**. **Note:** This is possible only when the account is in the **Managed** state. • **Completed**: Resource discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the account is in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Completed resource discovery only implies completion of the discovery process by AppViewX on AWS. All resources may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. • The resource discovery status of all entities mapped to the account should be **Completed**. • **Not Applicable**: The resource discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved,** • for ACM and ELB resources, • for all existing devices and child accounts as part of data migration.
Cert Discovery Status	**Note:** Cert discovery status is not applicable for master accounts. For master accounts, the cert discovery status is set to **Not Applicable**. This field indicates the status of the certificate discovery for the individual entities belonging to a discovered account using the following values: • **Not started**: Certificate discovery for the entity is yet to begin **Note:** At this point, the resource discovery status of the associated account can be **Not started**, **In-Progress**, or **Completed**. • **In-Progress**: Certificate discovery for the entity by AppViewX in the customer's AWS environment is currently in progress. The status is **In-Progress** till the certificate discovery status for all accounts is either **Completed** or **Not Applicable**. • **Completed**: Certificate discovery by AppViewX in the customer's AWS environment is complete. **Note:** This is possible only when the certificate discovery status for all the entities associated with the account is **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Completed certificate discovery only implies completion of the discovery process by AppViewX on AWS. All certificates may not be discovered all the time. The count of resources discovered with respect to the total resources will be shown in detailed reporting. . • **Not Applicable**: The certificate discovery status is set to **Not Applicable**: • when **Status** = **Failed** or **Resolved** • for EC2 when no EC2 instances are discovered • for all existing devices and child accounts as part of data migration **Note:** The cert discovery status is based on the status of only those entities for which the cert discovery status is not **Not Applicable**.
Cert sync	Cert sync type (**Managed**, **Monitored**, **Ignored**) selected for the entity
State	Outcome of the device addition (**Success**, **Failed**)

AWS IAM Prerequisites for Master Account

Permissions for Discovering Child Accounts using Policy-based Discovery

Note: This is required if IAM Policy-based account discovery is enabled in AppViewX. This IAM user account should be dedicated for the AppViewX Platform.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:GetUserPolicy",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "iam:ListGroupsForUser",
      "iam:ListGroupPolicies",
      "iam:ListAttachedUserPolicies",
      "iam:ListAttachedGroupPolicies",
      "iam:ListUserPolicies",
      "iam:GetGroupPolicy",
      "iam:GetUser"
    ],
    "Resource": "*"
  }
 ]
}
```

Permissions for Discovering Child Accounts using AWS Organization Services

Note: The permissions mentioned below should be enabled in the account in which organization service is enabled.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Enabling Assume Role Access to all AWS Accounts

Note: This action helps to automatically discover CLM resources in the newly created cloud accounts without manual intervention. This is an optional action, required only if the user prefers to grant access to all the child accounts for the IAM user.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": [
    "arn:aws:iam::<child account 1>:role/<Assume-role>",
    "arn:aws:iam::<child account 2>:role/< Assume-role>",
    "arn:aws:iam::<child account 3>:role/< Assume-role>"
   ]
  }
 ]
}
```

Permissions for Enabling Assume Role Access for a Specific Child Account

Note: If a user prefers not to grant assume role access to all accounts, they can define the RoleARN of a specific child account in the IAM policy, as is shown in the policy below.

Note: This is mandatory when IAM Policy-based account discovery is enabled in AppViewX for child account discovery.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "Action": [
      "sts:AssumeRole"
    ],
    "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

Permissions for Enabling S3 Bucket Access to the AppViewX Platform

Note: The permissions mentioned below are required only if the EC2 service has been added in AppViewX. IAM role should be created in the account with S3 permissions where the S3 bucket resides.

Note: This permission is required when assume role access is granted only to a specific RoleARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::<child-account>:role/AppViewX-S3-Bucket-Access"
    }
  ]
}
```

Permissions for Accessing Organization Services to Discover AWS Accounts

Note: This permission is required when assume role access is granted only to a specific RoleARN.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: This permission enables AppViewX to discover the AWS accounts associated to a specific organization.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "sts:AssumeRole"
   ],
   "Resource": "arn:aws:iam::<child-account>:role/AppViewX"
  }
 ]
}
```

AWS IAM Prerequisites for Child Account

Permissions for Establishing a Trust Relationship in Child Accounts

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::master-account-number:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {}
  }
 ]
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Permissions for Managing SSM Permissions for the EC2 Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
   "ssm:DescribeDocument",
   "ec2:DescribeInstances",
   "s3:ListAllMyBuckets",
   "ssm:DescribeInstanceInformation",
   "ssm:GetDocument",
   "ssm:CreateDocument",
   "ssm:GetCommandInvocation",
   "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions for Managing SSM Permissions for EC2 Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeDocument",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ssmmessages:OpenControlChannel",
                "ec2messages:DeleteMessage",
                "ssm:UpdateInstanceInformation",
                "ec2messages:FailMessage",
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            "ssmmessages:OpenDataChannel",
            "ssm:GetDocument",
            "ssm:ListTagsForResource",
            "ec2messages:AcknowledgeMessage",
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ec2messages:SendReply"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:PutObject",
            "s3:GetEncryptionConfiguration",
            "s3:PutObjectAcl"
        ],
        "Resource": [
            "arn:aws:s3:::appviewx-s3/*",
            "arn:aws:s3:::appviewx-s3"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Onboarding Certificates for AWS Resources in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for AWS Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan is triggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	• **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **AWS**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Account type**	From the following options, select the AWS account type for certificate discovery: • **Stand-alone account sign-in** (In a stand-alone account, the user account and the resources are available in the same account.) • **Cross account sign-in** (In a cross-account resources are available across multiple accounts and users are given role-based access.)
***Select Account View**	**Note:** This field is displayed only when you've selected **Account type** = **Cross account sign-in**. From the given options, select one to specify if the discovery will be performed for the master account or for the child accounts.
***Select Filter Type**	**Note:** This field is enabled when: • • **Account type** = **Stand-alone account sign-in** • **Account type** = **Cross account sign-in** AND **Select Account View** = **Child Account**. From the following options, select one to specify how the discovery results should be filtered: • **Account View** • **Service View**
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. b. Select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are listed in the certificate inventory.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42 • urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional). • **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to AWS Resources with EC2 Integration

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for AWS Resources with EC2 Integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **AWS**.
Service Types	From the dropdown list, **EC2**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available AWS cloud devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate Location**	Certificates can be stored in either AWS Certificate Manager (**ACM**) or AWS Identity and Access Management (**IAM**).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the options given, select the required certificate location.
Certificate ARN	**Note:** This field is displayed when **Certificate Location** = **ACM**. The ARN (Amazon Resource Name) is a unique identifier assigned to each certificate that is managed by ACM. It is used to reference the certificate in API calls, policies, and so on. In this field, enter the ARN of the certificate to be pushed.
***Certificate File Name**	**Note:** This field is displayed when **Certificate Location** = **IAM**. In this field, enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For AWS, this field is enabled by default and is non-editable.

5. Enter the **Certificate Tags**.
   A certificate tag is a label that you can assign to a certificate. To capture any details relevant to a certificate, you can associate certificate tags with a certificate. Certificate tags are key-value pair attributes that you can pass when you assume an IAM role or federate a user in AWS STS. These tags will be pushed along with the certificate to the endpoints. On certificate discovery, the tags associated with the certificate will be populated in the certificate inventory.

   To enter the certificate tags:

   a. **Enter Key** and **Enter Value**, in the respective fields, for the tag.

   b. Click **Add**.
      The tag, as a key-value pair, is listed in the table shown below the fields.

6. Enter/Select the **Push Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script.
Post - Push Script File Name	Enter the file name of the post push script.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

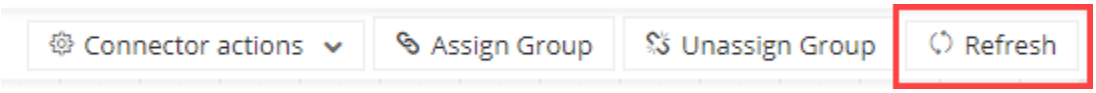
   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

- Create an IAM user in your AWS account.
- Create access keys for the root user.
- Create IAM policies using the JSON editor.
- Accessing member accounts.
- Using IAM roles for Amazon EC2 instances.
- Define custom IAM permissions for customer managed policies.

Automating CLM for Microsoft Azure Resources

Microsoft Azure is a comprehensive cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. It provides a wide range of cloud services, including those for computing, analytics, storage, and networking.

This section will guide you through the process of integrating Microsoft Azure with AppViewX, providing detailed steps, configuration guidelines, and automation techniques for the following services:

- With Key Vault Integration
- With Application Gateway Integration
- With Virtual Machines Integration
- With App Service Integration
- With Enterprise Application Integration
- With API Management Integration
- With App Registration Integration
- With Front Door Integration

With Key Vault Integration

This document will guide you through the process of integrating Azure Key Vault with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure Key Vault

The Azure Key Vault is a key management solution from Microsoft that offers the following features:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Secrets Management: The key vault can be used for securely storing and managing access to tokens, passwords, API keys, and other secrets.
- Key Management: The key vault simplifies the creation and management of encryption keys used for data encryption.
- Certificate Management: Azure key vault simplifies the certificate lifecycle management of TLS/SSL certificates

Prerequisites for Onboarding Azure Key Vault Settings in AppViewX

- Ensure that a key vault instance is created in your Microsoft Azure account. For link(s) to the corresponding Microsoft Azure documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

Certificates

```
{
  "properties": {
    "roleName": "AppViewX_KeyVault_Role",
    "description": "",
    "assignableScopes": [
      "/subscriptions/000-000-000-0000-000"
    ],
    "permissions": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    {
      "actions": [
        "Microsoft.KeyVault/vaults/read"
      ],
      "notActions": [],
      "dataActions": [
        "Microsoft.KeyVault/vaults/certificates/import/action",
        "Microsoft.KeyVault/vaults/certificates/create/action",
        "Microsoft.KeyVault/vaults/certificates/update/action",
        "Microsoft.KeyVault/vaults/certificates/read"
      ],
      "notDataActions": []
    }
  ]
 }
}
```

Secrets

```
{
 "properties": {
  "roleName": "AppViewX_KeyVault_Secret_Role",
  "description": "",
  "assignableScopes": [
    "/subscriptions/000-000-000-0000-000"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.KeyVault/vaults/secrets/read"
      ],
      "notActions": [],
      "dataActions": [
        "Microsoft.KeyVault/vaults/secrets/setSecret/action",
        "Microsoft.KeyVault/vaults/secrets/getSecret/action",
        "Microsoft.KeyVault/vaults/secrets/readMetadata/action"
      ],
      "notDataActions": []
    }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
  ]
 }
}
```

Onboarding Azure Settings in AppViewX for Key Vault

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. To validate the credential details entered above, click **Validate Credential**.

> **Note:** The option to **Validate Credential** is displayed only for a multi subscription account type.

Access to the **Discover Resources** section is enabled only after the credentials have been validated.

8. Enter/Select the details needed to **Discover Resources**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **Key Vault** to map the service to the Azure setting.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Subscription Onboarding State	Subscription onboarding refers to integrating an Azure subscription with AppViewX. You can choose to onboard all subscriptions at once or onboard only selected ones. From the following options, select a state for onboarding subscriptions discovered from the Azure organization: • **Managed**: Enables subscription onboarding, allowing Azure cloud resource and certificate discovery instantly • **Unmanaged**: Disables subscription onboarding, preventing resource and certificate discovery for these projects. After you have fetched all subscriptions belonging to these projects, you can select individual subscriptions for onboarding, as explained here.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the General Information section

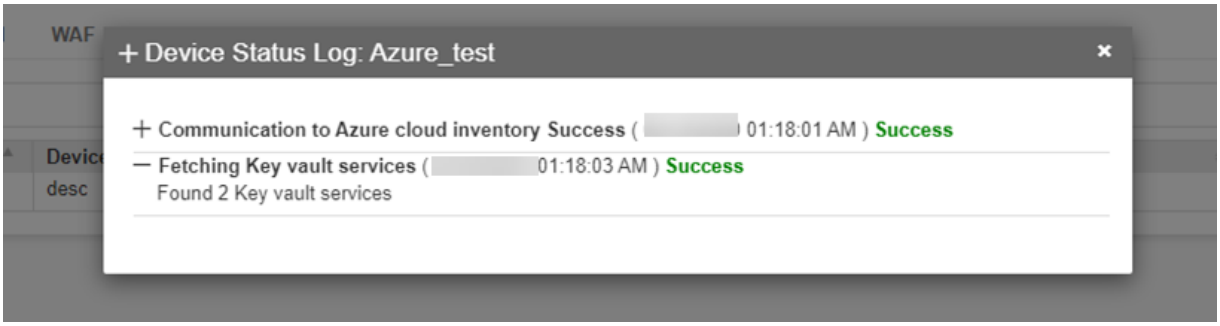
Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

9. For a multi subscription account, after specifying the details for resource discovery, click **Fetch Subscriptions**.
   a. From the subscriptions table, select the checkbox corresponding to the subscription(s) you want to manage.
   b. From the **Actions** dropdown menu, select **Manage**.
10. From **Additional attributes**, for the **Key Vault** service, select the user permission for **Cert sync** from the following options:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
- **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
- **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.

11. Click **Save**.
12. Return to the **Device :: Cloud** page.
13. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.



14. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure Key Vault

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure Key Vault

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **Key Vault**
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Keyvault Object Type	This fied is displayed when **Service Type** = **Key vault**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the key vault object to which the certificate will be pushed: • **Certificates** (The Azure key vault can store x509 certificates for securing communications and establishing the identity of services.) • **Secrets** (The Azure key vault secret is a secure object used for storing sensitive information, such as passwords and cryptographic keys.)
Certificate Status Enabled	This field is displayed only when **Keyvault Object Type** = **Secrets**. To enable the certificate after it is pushed to the target system, select **Yes**.
Set activation date	This field is displayed only when **Keyvault Object Type** = **Secrets**. To set an activation date for the certificate being pushed: a. Select the **Set activation date** checkbox. b. Use the calendar widget and time zone dropdown list to set the date and time for the certificate activation.
Set expiration date	This field is displayed only when **Keyvault Object Type** = **Secrets**. To set an expiration date for the certificate being pushed: a. Select the **Set expiration date** checkbox. b. Use the calendar widget and time zone dropdown list to set the date and time for the certificate expiry.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For Azure, this field is enabled by default and is non-editable.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

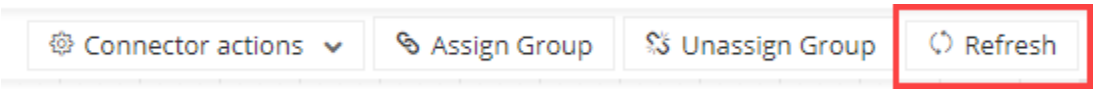
   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.

The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Create an Azure Key Vault using the Azure Portal.
- Configure managed identities on Azure virtual machines.

With Application Gateway Integration

This document will guide you through the process of integrating Azure Application Gateway with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure Application Gateway

The Azure Application Gateway is a web traffic load balancer that helps to optimize and secure web applications traffic. The application gateway operates at the application layer of the OSI model and makes routing decisions based on attributes of an HTTP request, for example the URI path or the host headers.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Prerequisites for Onboarding Azure Application Gateway Settings in AppViewX

- Ensure that an application gateway instance is created in your Microsoft Azure account. For link(s) to the corresponding Microsoft Azure documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

```
{
   "properties": {
      "roleName": "AppViewX_AppGW_Permission",
      "description": "",
      "assignableScopes": [
         "/subscriptions/000-000-000-0000-000"
      ],
      "permissions": [
         {
            "actions": [
               "Microsoft.Network/applicationGateways/write",
               "Microsoft.Network/applicationGateways/read",
               "Microsoft.Network/applicationGatewayAvailableSslOptions/predefinedPolicies/read",
               "Microsoft.Network/applicationGatewayAvailableSslOptions/read",
               "Microsoft.Network/virtualNetworks/subnets/join/action",
               "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
    ]
  }
}
```

Onboarding Azure Settings in AppViewX for Key Vault

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. To validate the credential details entered above, click **Validate Credential**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The option to **Validate Credential** is displayed only for a multi subscription account type.

Access to the **Discover Resources** section is enabled only after the credentials have been validated.

8. Enter/Select the details needed to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **Application Gateway** to map the service to the Azure setting.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Subscription Onboarding State	Subscription onboarding refers to integrating an Azure subscription with AppViewX. You can choose to onboard all subscriptions at once or onboard only selected ones. From the following options, select a state for onboarding subscriptions discovered from the Azure organization: • **Managed**: Enables subscription onboarding, allowing Azure cloud resource and certificate discovery instantly • **Unmanaged**: Disables subscription onboarding, preventing resource and certificate discovery for these projects. After you have fetched all subscriptions belonging to these projects, you can select individual subscriptions for onboarding, as explained here.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. For a multi subscription account, after specifying the details for resource discovery, click **Fetch Subscriptions**.
   a. From the subscriptions table, select the checkbox corresponding to the subscription(s) you want to manage.
   b. From the **Actions** dropdown menu, select **Manage**.
10. From **Additional attributes**, for the **Application Gateway** service, select the user permission for **Cert sync** from the following options:
    - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
    - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
    - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
11. Click **Save**.
12. Return to the **Device :: Cloud** page.
13. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.
14. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure Application Gateway

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure Application Gateway

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **Application Gateway**
Target Profile	Select the app service target profiles to which the certificate will be pushed.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Certificate Push Type	Select one from the following options: • **Upload a Certificate to Gateway**: • **Replace/Update existing Certificate in Gateway**:
Certificate Location	For the **Azure Application Gateway**, from the following options, select where the certificate will be stored after it is pushed: • **Upload directly to Application Gateway**: Upload certificates directly to the Application Gateway • **Choose from Azure Key Vault**: Store certificates in Azure Key Vault and then reference them in the Application Gateway configuration.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For Azure, this field is enabled by default and is non-editable.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

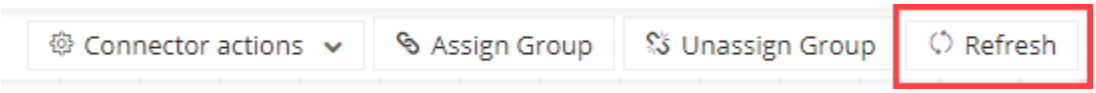
   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.
   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.
   c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

d. Click **Save**.

The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Create an Azure Application Gateway using the Azure Portal.
- Configure managed identities on Azure virtual machines.

With Virtual Machines Integration

This document will guide you through the process of integrating Azure Virtual Machines with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

> **Important:** Please note the following **limitations** for Azure virtual machines:
>
> - Currently, only the Linux-based VMs (and not Windows-based VMs) are discovered.
> - The discovered/onboarded VMs are listed in the server device inventory.
>
> You are required to manually update the VM credentials in the server inventory to proceed with certificate lifecycle management for the VM.
>
> To access the server inventory, Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management** and open the **Server** tab.

Microsoft Azure Virtual Machines

Azure Virtual Machines (VMs) are scalable and flexible computing resources provided by Microsoft Azure. They enable users to run virtualized Windows or Linux servers in the cloud. Azure VMs allow you to

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

quickly deploy and manage virtualized infrastructure to support various applications, workloads, and services.

Prerequisites for Onboarding Azure Virtual Machine Settings in AppViewX

- Ensure that a virtual machine instance is created in your Microsoft Azure account. For link(s) to the corresponding Microsoft Azure documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

```
{
 "properties": {
  "roleName": "AppViewX_VirtualMachine_Role",
  "description": "",
  "assignableScopes": [
   "/subscriptions/000-000-000-0000-000"
  ],
  "permissions": [
   {
    "actions": [
     "Microsoft.Compute/virtualMachines/read",
     "Microsoft.Network/networkInterfaces/read"
    ],
    "notActions": [],
    "dataActions": [],
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
      "notDataActions": []
    }
   ]
  }
}
```

Onboarding Azure Settings in AppViewX for Virtual Machines

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. To validate the credential details entered above, click **Validate Credential**.

Note: The option to **Validate Credential** is displayed only for a multi subscription account type.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Access to the **Discover Resources** section is enabled only after the credentials have been validated.

8. Enter/Select the details needed to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **Virtual Machines** to map the service to the Azure setting. Starting v2024.1.0.0, Linux-based as well as Windows-based VMs can be discovered. For instructions on managing the Linux-based/Windows-based server devices onboarded as VMs, click here.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Subscription Onboarding State	Subscription onboarding refers to integrating an Azure subscription with AppViewX. You can choose to onboard all subscriptions at once or onboard only selected ones. From the following options, select a state for onboarding subscriptions discovered from the Azure organization: • **Managed**: Enables subscription onboarding, allowing Azure cloud resource and certificate discovery instantly • **Unmanaged**: Disables subscription onboarding, preventing resource and certificate discovery for these projects. After you have fetched all subscriptions belonging to these projects, you can select individual subscriptions for onboarding, as explained here.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. For a multi subscription account, after specifying the details for resource discovery, click **Fetch Subscriptions**.
   a. From the subscriptions table, select the checkbox corresponding to the subscription(s) you want to manage.
   b. From the **Actions** dropdown menu, select **Manage**.
10. From **Additional attributes**, for the **Virtual Machine** services, select the user permission for **Cert sync** from the following options:
    - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
    - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
    - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
11. Click **Save**.
12. Return to the **Device :: Cloud** page.
13. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.
14. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Managing Server Devices Onboarded as Azure Virtual Machines

The discovered/onboarded VMs are listed in the server device inventory.

To access the server device inventory, Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management** and open the **Server** tab.

Once the server device is onboarded, you are required to manually update the VM credentials in the server inventory to proceed with certificate lifecycle management for the VM.

To do this:

1. Go to the server device inventorty.
2. On the **Device :: Server** page, click the device **Name** to modify the device details.
   You will be redirected to the **Device details** page.
3. In the **Credentials** section, update the device credentials.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For field descriptions and other details, refer from the following links:

- Configuring Linux Server
- Configuring Microsoft Server

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	<u>To search for a resource</u>: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type** iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. <u>To add an existing resource to the list</u>: a. Click . b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. <u>To delete a resource from the list</u>: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	OR Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure Virtual Machines

> **Important:** Refer to the pre- and post-push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Adding an Application Connector for Azure Virtual Machines

For Linux-based Virtual Machines

Important: If the certificate is generated with CSR generation at endpoint, if an application connector is created for the certificate, the following fields will be auto-populated/selected and cannot be modified:

- **Category**
- **Vendor**
- **Key Location**
- **Private key in Device**

Additionally, the available profiles will be filtered for the device profile selected at the time of certificate enrollment here.

1. On the client (or) server certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **LinuxServer**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

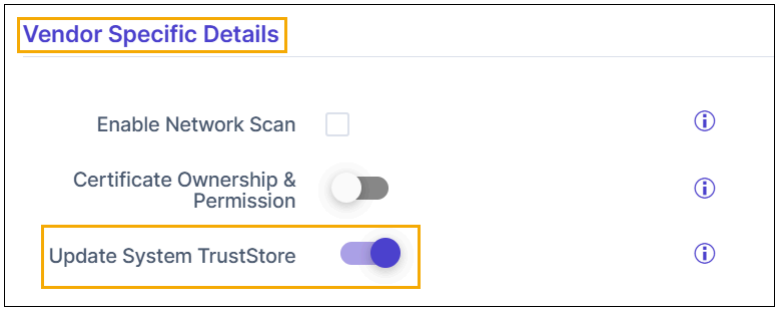
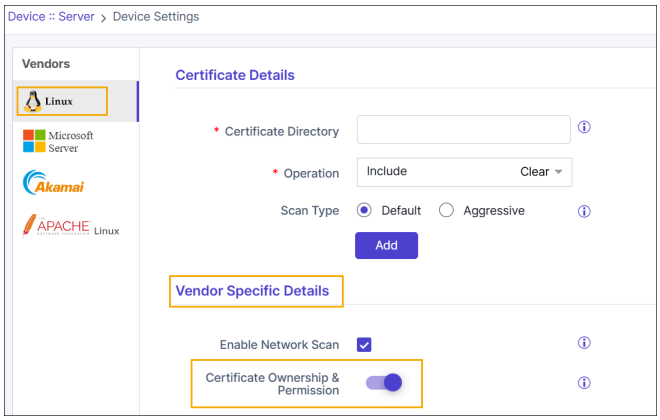
Based on the information entered here, the **SSL templates** section is populated with the list of available Linux Server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   You can use the **Available Devices** dropdown list to filter devices based on functionality.
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
Enable Truststore Update	This field is displayed for all **PEM** certificate types. Click the radio button to enable the Update System TrustStore option for root and intermediate certificates. **Note:** By default, this option is disabled. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** > **Vendor Specific Details** section > **Update System TrustStore**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	
Certificate Ownership & Permission	Enable the toggle button to customize the certificate ownership and define the file permissions for the certificates. **Note:** The toggle button will be enabled by default for Linux devices if it is activated in the Device Settings under the **CERT+** > **ADMINISTRATION** > **Device Management** > **Server** > **Device Settings** > **Vendor Specific Details** section > **Certificate Ownership & Permission**.  Field descriptions for the Certificate Ownership & Permission Details
Custom Push	This field is displayed for all **PEM** and **DER** certificate types. From the following options, select the method of pushing certificates: • **Chain**: The full certificate chain, which includes the end, intermediate, and root certificates, will be pushed to the server. • **Issuer & Server**: The server's certificate and its issuer's certificates will be pushed to the server. • **Server Only**: Only the server's certificate will be pushed to the server.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KDB File Name**	Enter the name of the KDB certificate file that will be pushed to the IBMClient server.
***KDB password**	Enter the password required to access the KDB certificate file.
Server Certificate Label	This field is disabled when the **Private key in device** checkbox is selected. Enter the label for the server certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. For the Linux Server, this feature is enabled by default and the field is non-editable.
Intermediate Certificate Label	If an intermediate certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Root Certificate Label	If a root certificate is available in the KDB file, the system will retain the existing label. The given label name will not be used.
Certificate Location	This field is displayed for all PEM, DER and PKCS#7 certificates. Enter the path to the location on your local system where the certificate file to be pushed is stored.
Key Location	This field is displayed for all PEM, DER and PKCS#7 certificates. The private key associated with a certificate is stored in a key file. In the **Key Location** field, enter the path to the location on your local system where the private key file for the certificate to be pushed is stored.
***KeyStore Location**	This field is displayed for the PKCS#12 and JKS certificates. A keystore is a repository used for storing private keys and certificates. In the **KeyStore Location** field, enter the path to the location on your local system where the keystore file, for the certificate to be pushed, is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***KeyStore Password**	This field is displayed for the PKCS#12 and JKS certificates. Enter the password required to access the keystore file for the certificate to be pushed.
***Alias Name**	This field is displayed for the PKCS#12 and JKS certificates. Enter the certificate alias assigned in the CSR generated for requesting/enrolling the certificate.
Truststore Location	In the **Truststore Location** field, enter the path to the location on your local system where the truststore file, for the certificates to be pushed, is stored. **Note:** Truststore Location can be specified without the file extension as well.
Truststore password	This field is displayed for the JKS certificates. Enter the password required to access the truststore file for the JKS certificate to be pushed.
Private key in device	If the private key associated with the certificate being pushed has been stored on a hardware device, select this checkbox.

Field descriptions for the Certificate Ownership & Permission Details

Field	Description
Owner	Enter the username for certificate ownership on the target device.
Owner Permission	Select the owner permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).
User Group	Enter name of the user group that requires access to the certificate.
User Group Permission	Select the group permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Other User Permission	Select the other user permission level from the dropdown list. • Read (r) • Read-Write (rw) • Read-Write-Execute (rwx).

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

For Windows-based Virtual Machines

Prerequisistes: When adding connectors using the Exchange Server, note the following points:

- During Microsoft Server device addition ensure that the username is added with the domain in the format—<username>@<domain>.
- The **iisreset.exe** file is expected at the default location. (C:\Windows\System32) to support IIS Service restart.
- For the certificate being enrolled, **Country name** must be provided in order to renew the certificate.

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **Microsoft Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **Server selection** section is populated with the list of available ABAP server devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, from the dropdown list, select one of the following options:
   - **MS Server**
   - **Exchange Server**
   - **Windows Gateway**

   Note: If you have selected **Exchange Server**, profiles will be displayed in the format, **Server type : Service name : Node details**.

4. Under **Server selection**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
5. Enter the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For MS Server: Field descriptions for the Certificate Details

Field	Description
Location Type	From the following options, select the location to which the certificate will be pushed: • **File System** (a storage location on your computer) • **Certificate Store** (a specialized location within the operating system for managing digital certificates)
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Credential Type**	This field is displayed for the JKS certificates. From the dropdown list, select the source of the access credentials.
***Push Location**	Enter the endpoint where the certificate will be pushed. This can be a network location or directory on the server, or a URL from where the server can retrieve the certificate.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
***Key File Name**	This field is displayed for the **PEM**, **DER**, and **PKCS#7** certificates. The private key associated with a certificate is stored in a key file. Enter the name of the file that contains the private key associated with the certificate to be pushed. The file extension **.key** is automatically populated.
***PFX Password**	This field is displayed when **Certificate Type** = **PKCS#12 (*.pfx)** and **PKCS#12 (*.p12)**. Enter the password that will be required to access the **.pfx** and the **.p12** certificate files.
***KeyStore Password**	This field is displayed for JKS certificate types. Enter the password required to access the keystore that contains the JKS certificate to be pushed.
Alias Name	This field is displayed for the PKCS#12 and CERTDB certificate types.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Enter the certificate alias assigned in the CSR generated for requesting/ enrolling the certificate.
Private key entry password	This field is displayed for the JKS certificates. Enter the password required to decrypt the private key associated with the certificate.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
***Intermediate Certificate Alias Name 1**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. This field is not displayed for the JKS certificate types. Enter the alias name of the intermediate certificate file.
***Root Certificate Alias Name**	This field is displayed only when **Push Root and Intermediate Certificates** is enabled. Enter the alias name of the root certificate file.

For Exchange Server: Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	The certificate type is defaulted to the following values • For AppViewX CSR generation - certificates which have private key, **PKCS#12(*.p12)** is the supported certificate format. • For Endpoint CSR generation **PKCS#7(*.p7b)** is the supported certificate format.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The password field in not set for **PKCS#12(*.p12)** since its a transactional password and handled by AppViewX.
***Friendly Name**	• For **PKCS#12(*.p12)** it is the user specified input. • For **PKCS#7(*.p7b)** certificate type, the friendly name is the common name of the certificate specified at the time of Endpoint CSR generation. During the push operation the common name is populated in the friendly name field (it is not editable).
Services	From the dropdown list, select one from the following services: • **POP** • **IIS** • **SMTP** • **IMAP**
Restart Service	This field is displayed only when **Services** = **IIS**. To restart the IIS service after the certificate is pushed, to ensure all changes have taken effect as required, select this checkbox.

For Windows Gateway: Field descriptions for the Certificate Details

Field	Description
Location Type	The **Certificate Store** option is selected by default—a specialized location within the operating system for managing digital certificates. (**File system** is disabled).
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox. **Note:** Root and intermediate names cannot be entered for this CSR/Certificate. If auto-push is enabled for CSR, try again after the certificate is generated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings This is applicable for all service/devices such as Microsoft Server, Microsoft Exchange Server, Windows Gateway.

6. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Overwrite	The **Overwrite** option is used to specify if existing certificates on the target system will be overwritten with the certificate being pushed. If this option is enabled, the certificate being pushed will overwrite any existing certificates with the same identifier on the target system. This will also ensure that only the latest version of the certificate is available on the target system. If it is disabled, the push operation will fail in the event of conflicts with the certificates on the target system.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.
Secure Push	The **Secure Push** option ensures that the certificate is pushed to the target system securely, protected from any unauthorized access.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

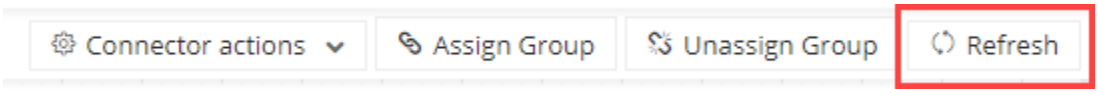
The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Create a Linux Virtual Machine using the Azure Portal.
- Create a Windows Virtual Machine using the Azure Portal.
- Configure managed identities on Azure virtual machines.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

With App Service Integration

This document will guide you through the process of integrating Azure App Service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure App Service

App Services is a fully managed platform for building, deploying, and scaling web apps, mobile app backends, and RESTful APIs.

Prerequisites for Onboarding Azure App Service Settings in AppViewX

- Ensure that an app service instance is created in your Microsoft Azure account. For link(s) to the corresponding Microsoft Azure documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

```
{
    "properties": {
        "roleName": "AppViewX_App_Service_Permission",
        "description": "",
        "assignableScopes": [
            "/subscriptions/000-000-000-0000-000"
        ],
        "permissions": [
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
        {
            "actions": [
                "Microsoft.Web/sites/Read",
            "Microsoft.Web/sites/Write",
            "microsoft.web/sites/publiccertificates/read",
                "microsoft.web/sites/publiccertificates/write",
                "Microsoft.Web/sites/restart/Action",
                "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
    ]
  }
}
```

Onboarding Azure Settings in AppViewX for App Service

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. To validate the credential details entered above, click **Validate Credential**.

> **Note:** The option to **Validate Credential** is displayed only for a multi subscription account type.

Access to the **Discover Resources** section is enabled only after the credentials have been validated.

8. Enter/Select the details needed to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **App Service** to map the service to the Azure setting.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Subscription Onboarding State	Subscription onboarding refers to integrating an Azure subscription with AppViewX. You can choose to onboard all subscriptions at once or onboard only selected ones.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select a state for onboarding subscriptions discovered from the Azure organization: • **Managed**: Enables subscription onboarding, allowing Azure cloud resource and certificate discovery instantly • **Unmanaged**: Disables subscription onboarding, preventing resource and certificate discovery for these projects. After you have fetched all subscriptions belonging to these projects, you can select individual subscriptions for onboarding, as explained here.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Field descriptions for the General Information section

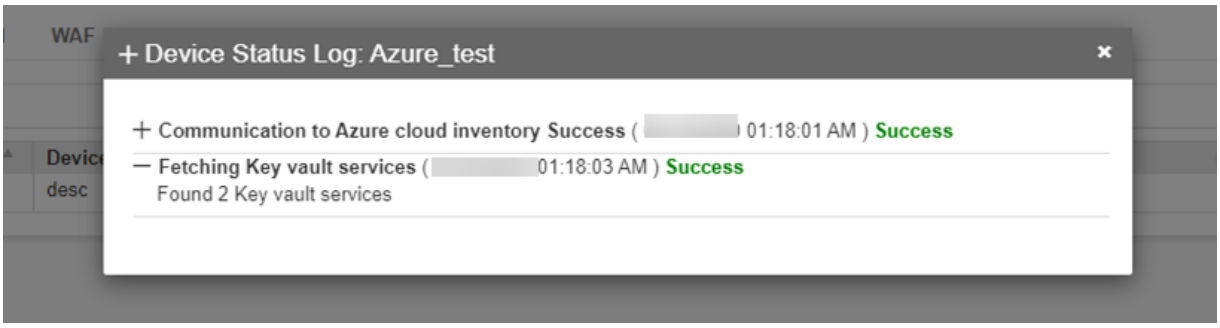
Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

9. For a multi subscription account, after specifying the details for resource discovery, click **Fetch Subscriptions**.
   a. From the subscriptions table, select the checkbox corresponding to the subscription(s) you want to manage.
   b. From the **Actions** dropdown menu, select **Manage**.
10. From **Additional attributes**, for **App Service**, select the user permission for **Cert sync** from the following options:
    - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
    - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
    - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
11. Click **Save**.
12. Return to the **Device :: Cloud** page.
13. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



14. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type** iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click . b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

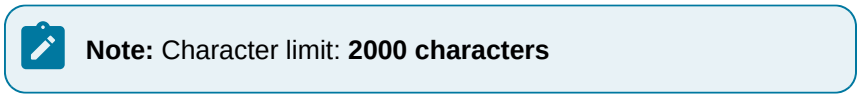
Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field.  **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure App Service

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure App Service

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **App Service**
Target Profile	Select the app service target profiles to which the certificate will be pushed.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.
Certificate Location	For the **Azure App Service**, from the following options, select where the certificate will be stored after it is pushed: • **Upload a Certificate to App Service** • **Replace/Update existing Certificate in App Service**: If a version of the certificate being pushed already exists in the App Service, it will be replaced/ updated with the version that will be pushed via this connector.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox. For Azure, this field is enabled by default and is non-editable.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   > **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

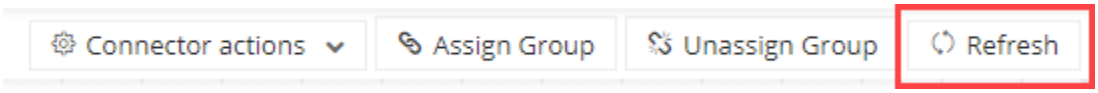
   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
    a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
    The **Group** page is displayed.
    b. From the **Name** field, select the required certificate group.
    The **Group : Modify : <group name>** page is displayed.
    c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
    d. Click **Update**.
2. To enable auto push for the certificate connector:
    a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
    To add an application connector, follow the instructions given here.
    b. From the menu displayed, click **Edit**.
    The **Edit Application Connector** pop-up is displayed.
    c. Select the **Push automatically** checkbox.

    > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

    d. Click **Save**.
    The holistic view of the selected certificate is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Getting Started with the Azure App Service.
- Configure managed identities on Azure virtual machines.

With Enterprise Application Integration

This document will guide you through the process of integrating Azure Enterprise Application with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure Enterprise Application

The Enterprise Application service in Azure Active Directory (Azure AD) is used for managing identity and access for SaaS applications, custom apps, and other resource.

Prerequisites for Onboarding Azure Enterprise Application Settings in AppViewX

- Ensure that an enterprise application instance is created in your Microsoft Azure account. For link(s) to the corresponding Microsoft Azure documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

  For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

The user should have access to the following Graph APIs:

- **Application.Read.All**
- **Application.ReadWrite.All**

Onboarding Azure Settings in AppViewX for Enterprise Application

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the details needed to **Discover Resources**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **Enterprise Application** to map the service to the Azure setting.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

8. Enter/Select values for the **Additional attributes** for the Enterprise Application service.

Field descriptions for the additional Enterprise Application attributes

Field	Description
Cert sync	To specify how certificates will be handled after discovery, select one from the following options: • **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions. • **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates. • **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
Discover Inactive Certificates	The Enterprise Application service has an active certificate associated with it, which is the default certificate used for securing communication, authentication, and encryption. The rest of the certificates associated with this service are categorized as inactive certificates. To enable discovery of inactive certificates along with the active certificate associated with the selected service(s), enable the **Discover Inacrive Certificates** toggle button.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Notify For	You can choose to receive email notifications every time: • a certificate is pushed to the Enterprise Application service • a certificate is made active certificate while being pushed to the Enterprise Application service To receive email notifications: a. Enable the **Notify For** toggle button. b. To receive notifications when a certificate is pushed, select **Push**. To receive notifications when a certificate is made active certificate while being pushed, select **Make Certificate Active**.
***Email Alert Template**	**Note:** This field is displayed only when **Notify For** is enabled. From the list of predefined email templates in the dropdown list, select the email template that will be used to send the alert. By default, the **Azure SSO Template** is selected. **Note:** To view the predefined templates, go to **Platform** > **System Administration** > **Themes & Personalization** > **Email attachment customization**. The predefined templates are listed in the **Email Template** section.
***Email Subject**	**Note:** This field is displayed only when **Notify For** is enabled. Enter a custom email subject for the notification email.
Attach Certificates to Email Body	**Note:** This field is displayed only when **Notify For** is enabled. If you need the relevant certificate(s) attached to the notification email, from the following options, select the format in which the certificate will be shared: • **Include as Content** The email body includes the contents of the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed is an inactive certificate, the email will also include instructions for manually making it the active certificate. • **Include as Downloadable Link** (to include The email body includes a link for downloading the certificate. Clicking the link will redirect you to the holistic view of the certificate, from where you can download the certificate.
**: Mandatory fields*	

9. Click **Save**.
10. Return to the **Device :: Cloud** page.
11. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.
12. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure Enterprise Application

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure Enterprise Application

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **Enterprise Application**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed. For the Enterprise Application service, by default, the **PKCS#12 (*.pfx)** certificate type is selected and the field is disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Make Certificate Active	To make the certificate being pushed the active certificate for the Enterprise Application service, select this checkbox. An active certificate is the default certificate used for securing communication, authentication, and encryption. The rest of the certificates associated with this service are categorized as inactive certificates.
Notification Email Addresses	To enter email addresses that will be notified when this certificate is pushed and/or made active: a. Click . b. Enter the required email address and press **Enter**. c. To add multiple email addresses, repeat steps **a** and **b**. Alternatively, you can use the search field to add an already entered email address.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   > **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

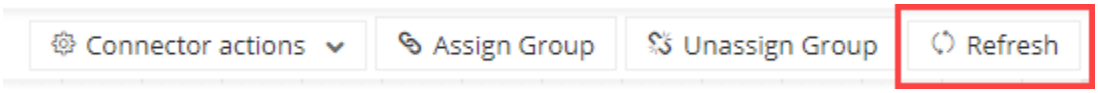
   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Managing Enterprise Application Certificates

Starting v2024.0.1.0, self-signed certificates discovered from the Enterprise Application service can be:

- Renewed
- Made active

Renewing an Enterprise Application Self-Signed Certificate

To renew an Enterprise Application Self-Signed Certificate,

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the Enterprise Application Self-Signed Certificate that you want to renew.
   The holistic view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Renew**.
4. In the **Renew** dialog box:
   a. Enter the new **Validity** for the renewed certificate.
   b. To make the certificate active, select the **Make Certificate Active** checkbox.
5. Click **Renew**.
   A request ID, which is the work order ID, is generated automatically, and work order status is displayed adjacent to the certificate in the holistic view. If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
6. In the holistic view, click **Approve** to proceed.
   The **Approve** dialog box is displayed.
7. Enter your comments in the text field.

   Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

8. Click **Yes**.
   Once the approval process is complete, the **Implement** option is displayed in the holistic view.
9. Click **Implement**.
   The **Implement** dialog box is displayed.
10. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
11. Click **Yes**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

The renewal process is triggered. After renewal is completed:

- Workflow status is updated to **Completed**.
- A notification email is sent.

12. To see if the certificate has been made active (if you selected the checkbox), hover over the application connector for the certificate.
    If the certificate is active, the **Is Active** field in the tooltip text is set to **Yes**.

Making an Enterprise Application Self-Signed Certificate Active

There are two ways in which you can make an Enterprise Application self-signed certificate active.

- By selecting the **Make Certificate Active** checkbox from the **Renew** dialog box for the self-signed certificate

  The instructions for this are given here.

- By selecting the **Make Certificate Active** option from the **More** menu in the holistic view

  The instructions for this are given below.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** > **Server**.
   The **Server Certificate** page is displayed.
2. Select the Enterprise Application Self-Signed Certificate that you want to make active.
   The holistic view for the selected certificate is displayed.
3. From the **(More)** menu for the certificate, click **Make Certificate Active**.
4. To see if the certificate has been made active, hover over the application connector for the certificate.
   If the certificate is active, the **Is Active** field in the tooltip text is set to **Yes**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

   b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

   c. Select the **Push automatically** checkbox.

   > **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

   d. Click **Save**.
   The holistic view of the selected certificate is displayed.

   > **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

   > **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

References

- Add an Enterprise Application.
- Configure managed identities on Azure virtual machines.

With API Management Integration

This document will guide you through the process of integrating the Azure API Management service with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure API Management

The API Management service helps create, manage, secure, and monitor APIs. It provides a centralized platform for API publishers to control their APIs, while enabling developers to consume them in a secure and efficient manner.

Its key features include:

- API Gateway that routes all incoming requests to the appropriate backend services
- Developer Portal that can be customized to help developers discover and access APIs
- API versioning with revision tracking
- Authentication and authorization mechanisms for secure access control to APIs
- Rate limiting and throttling to protect backend services from excessive or abusive traffic
- Analytics and monitoring
- Policy Engine to implement additional logic at the API Gateway

Prerequisites for Onboarding Azure API Management Settings in AppViewX

- Ensure that a API management instance is created in your Microsoft Azure account. For link(s) to the corresponding Microsoft Azure documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
- A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
- Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

  For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

```
{
   "properties": {
      "roleName": "AppViewX_APIMngmnt_Permission",
      "description": "",
      "assignableScopes": [
         "/subscriptions/000-000-000-0000-000"
      ],
      "permissions": [
         {
            "actions": [
               "Microsoft.ApiManagement/service/certificates/read",
               "Microsoft.ApiManagement/service/certificates/write",
               "Microsoft.ApiManagement/service/certificates/delete",
               "Microsoft.ApiManagement/service/certificates/refreshSecret/action"
               "Microsoft.ApiManagement/service/read",
               Microsoft.ManagedIdentity/userAssignedIdentities/assign/action
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
         }
      ]
   }
}
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Onboarding Azure Settings in AppViewX for API Management

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. To validate the credential details entered above, click **Validate Credential**.

> **Note:** The option to **Validate Credential** is displayed only for a multi subscription account type.

Access to the **Discover Resources** section is enabled only after the credentials have been validated.

8. Enter/Select the details needed to **Discover Resources**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **Api Management** to map the service to the Azure setting.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Subscription Onboarding State	Subscription onboarding refers to integrating an Azure subscription with AppViewX. You can choose to onboard all subscriptions at once or onboard only selected ones. From the following options, select a state for onboarding subscriptions discovered from the Azure organization: • **Managed**: Enables subscription onboarding, allowing Azure cloud resource and certificate discovery instantly • **Unmanaged**: Disables subscription onboarding, preventing resource and certificate discovery for these projects. After you have fetched all subscriptions belonging to these projects, you can select individual subscriptions for onboarding, as explained here.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

9. For a multi subscription account, after specifying the details for resource discovery, click **Fetch Subscriptions**.
   a. From the subscriptions table, select the checkbox corresponding to the subscription(s) you want to manage.
   b. From the **Actions** dropdown menu, select **Manage**.
10. From **Additional attributes**, for the **Api Management** service, from the following options, select the user permission for **Cert sync**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
- **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
- **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.

11. Click **Save**.
12. Return to the **Device :: Cloud** page.
13. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.
14. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type** iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.

5. In the **After Discover** section, enter/select the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Once the certificates are discovered, you can view them in the certificate inventory.

To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure API Management

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure API Management

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. On the certificate holistic view, click **Add Connector**.

2. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **Api Management**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
4. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.
***Certificate File Name**	Enter the file name of the certificate to be pushed. The file extension is auto-populated based on the **Certificate Type** selected.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Push Type	Certificate push type specifies the mechanism that will be used for pushing certificates to the targeted service. For the Azure Api management service, certificate push type has the following values: • **Upload a Certificate to Api Management** (for uploading a new certificate) • **Replace/Update existing Certificate in Api Management** (for renewing/ replacing an existing certificate) **Important:** For the Azure Api management service, this field is disabled for editing and the **Upload a Certificate to App Service** is selected by default.
Certificate Location	From the following options, select where the certificate will be stored after it is pushed: • **Upload directly to Api Management**: Upload certificates directly to the Application Gateway • **Choose from Azure Key Vault**: Store certificates in Azure Key Vault and then reference them in the Api Management configuration.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

5. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

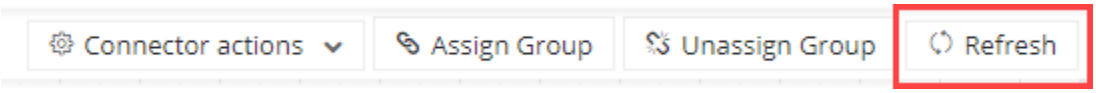
a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
b. If you select **Off**, set the date and time to schedule the certificate push.
c. Enter your comments in the text field and click **Yes**.

The work order status displayed beside the connector updates to **Push-Review In Progress**.

8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:
   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.
   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.
   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.
   d. Click **Update**.
2. To enable auto push for the certificate connector:
   a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
      To add an application connector, follow the instructions given here.
   b. From the menu displayed, click **Edit**.
      The **Edit Application Connector** pop-up is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.

The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Create a new Azure API Management Instance by using the Azure Portal.
- Configure managed identities on Azure virtual machines.

With App Registration Integration

This document will guide you through the process of integrating Azure App Registration with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure App Registration

The App Registration service enbales identity and access management, API security, and integration capabilities. It is used for registering and configuring applications for interactions with Azure services.

App Registration service is essential when you want to allow your application to authenticate users or access resources such as APIs in a secure way.

Its key features include:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Application Identity Management
- Authentication Support
- Access permissions and scope definition for APIs
- Multi-Tenant and Single-Tenant support
- Enterprise Application Integration
- Roles and Role-Based Access Control
- Token Issuance and Validation for Authentication and Authorization
- Auditing and Monitoring
- Conditional Access and Multi-Factor Authentication

Prerequisites for Onboarding Azure App Registration Settings in AppViewX

- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

The user should have access to the following Graph APIs:

- **Application.Read.All**
- **Application.ReadWrite.All**

Onboarding Azure Settings in AppViewX for App Registration

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. On the **Device :: Cloud** page, click + (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity**: [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**. From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the details needed to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **App Registration** to map the service to the Azure setting.
Subscription ID	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. Field descriptions for the **General Information** section
**: Mandatory fields*	

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

8. From **Additional attributes**, for the **App Registration** service, select the user permission for **Cert sync** from the following options:
   - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
   - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
   - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
9. Click **Save**.
10. Return to the **Device :: Cloud** page.
11. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.
12. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

   OR

   Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

   Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option. If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click Add Resource. b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click . **OR** Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall **Note:** • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

4. For the **EJBCA** certificate authority, enter the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure App Registration

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure App Registration

1. To create an application connector for pushing a certificate, go the holistic view of the certificate.
   To do this:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Go to (**Menu**) > **CERT+** > **Certificate Inventory** and select the required certificate category.

b. From the certificate inventory displayed, select the **Common Name** of the certificate you want to push.
The holistic view of the certificate is displayed.

2. On the certificate holistic view, click **Add Connector**.

3. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **App Registration**
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure devices already onboarded in AppViewX.

4. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required device(s), click .
The **Selected devices** list is updated automatically.
5. Enter/Select the **Certificate Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Certificate Details

Field	Description
***Certificate Type**	From the dropdown list, select the file type of the certificate to be pushed.

6. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

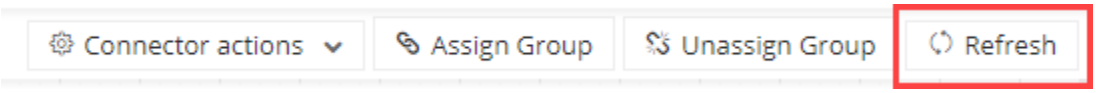
The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:** The **Push to Device** option is displayed only after an app connector is added to certificate.

The **Confirmation** dialog box is displayed.

4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Configure managed identities on Azure virtual machines.

With Front Door Integration

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

This document will guide you through the process of integrating Azure Front Door with AppViewX, providing detailed steps, configuration guidelines, and automation techniques.

Microsoft Azure Front Door

Azure Front Door is a modern, high-performance, and secure cloud Content Delivery Network (CDN) that serves as the global entry point for your applications. It optimizes traffic by routing users to the nearest edge location for faster, more reliable access, while built-in caching, acceleration, and a Web Application Firewall (WAF) provide enhanced performance and protection—making it ideal for global websites and SaaS applications.

Prerequisites for Onboarding Azure Front Door Settings in AppViewX

- Ensure that a Azure Front Door instance is created in your Microsoft Azure account. For link(s) to the corresponding Azure Front Door documentation, click here.
- If credentials for onboarding have to be fetched from a credential list in CyberArk:
  - Ensure that your Microsoft Azure access credentials are saved in your CyberArk account. For instructions on creating Azure access details in the CyberArk account , refer to the documentation here.
  - Ensure that CyberArk is integrated with AppViewX and a credential list is created. For instructions, refer to the documentation here.
- For using the Managed Identity credential type, ensure the following requirements are met:
  - The AppViewX Cloud Connector (CC) is installed on the target Azure VM.
  - A user-assigned or system-assigned Managed Identity is associated with the Azure VM.
  - Strict routing is enabled for the corresponding data center to ensure secure and consistent communication.

    For links to the complete Microsoft Azure documentation on configuring managed identities for Azure VMs, see the **References** section.

Permissions Required

```
{
   "properties": {
      "roleName": "AppViewX_FrontDoor_Permission",
      "description": "",
      "assignableScopes": [
         "/subscriptions/000-000-000-0000-000"
      ],
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    "permissions": [
      {
        "actions": [
          "Microsoft.Resources/subscriptions/resources/read",
          "Microsoft.Cdn/profiles/customDomains/read",
          "Microsoft.Cdn/profiles/secrets/read",
          "Microsoft.Cdn/profiles/customDomains/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Onboarding Azure Settings in AppViewX for Front Door

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   The **Device :: ADC** page is displayed.
2. From the **Device :: ADC** page, select **Cloud**.
3. On the **Device :: Cloud** page, click (**Add**).
   The **Device :: Cloud > Add** page is displayed.
4. On the **Device :: Cloud > Add** page, from the list of **Vendors**, select **Azure**.
5. Enter/Select the **Basic information**.

Field description for the Basic Information section

Field	Description
Configure Government Cloud	To configure Azure Government Cloud for this Microsoft Azure, turn on the **Configure Government Cloud** toggle. Azure Government Cloud is a specialized cloud computing platform provided by Microsoft, designed specifically for U.S. government agencies and their partners. While it offers the same core services as the commercial Microsoft Azure cloud, it offers additional complaince, security, and regulatory controls configured to meet the stringent security requirements of its primary use cases.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Country**	From the dropdown list, select the country for which the Azure Government Cloud is being configured. **Important:** In the current implementation, the Azure Government Cloud configuration is supported **only** for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and complaince as per the U.S. regulations.
***Account Type**	From the dropdown list, select one of the following values: • **Single Subscription** • **Multi Subscription** To understand the subscription types and the difference between them, click here.
***Account Name**	Enter the customer's unique account name. Constraints: • A duplicate account name should not exist in the cloud inventory. • The account name should include only alphanumeric and period (.) characters.
Description	Enter a description of the device to be added.
***Data center**	From the dropdown list, select the data center through which communication with the Certificate Authority will be established.
Proxy required	To use a proxy server for the communication, select this checkbox. Proxy settings configured in the **Platform** module will be used for communication. To read more on how proxy settings are configured and managed, click here.
**: Mandatory fields*	

6. Enter/Select the **Credential Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field description for the Credential Details section

Field	Description
***Credential type**	From the dropdown list, from the following options, select the authentication method that will be used for integrating Microsoft Azure with AppViewX: • **Manual Entry**: The required credentials will be entered manually. • **Credential List - CyberArk**: The required credentials will be retrieved from CyberArk, a Privileged Access Management (PAM) solution. • **Managed Identity** : [Read the Managed Identity prerequisites given above.] An Azure-assigned Managed Identity is used for Azure Active Directory (Azure AD) authentication, fetching tokens automatically without storing credentials in AppViewX. Managed Identity is an Azure-generated identity that allows resources to authenticate to Azure AD-protected services without storing credentials. At this time, the **Managed Identity** credential is not supported for an Azure Government Cloud environment.
***Tenant ID**	Enter the unique identifier (GUID) of your Azure Active Directory Tenant.
Managed Identity Type	This field is displayed only when **Credential type** = **Managed Identity**. From the dropdown list, from the following options, select how Managed Identity is provisioned and managed for the resource to be onboarded: • **User Managed**: Use when you need a standalone identity that can be assigned to one or more Azure resources and managed independently. • **System Managed**: Use when you want Azure to automatically create and manage an identity that is tied to a single resource's lifecycle.
***Client ID**	Enter your Azure client ID (application ID). For **Credential type** = **Managed Identity**, this field is displayed only when **Managed Identity Type** = **User Managed**. In this case, enter the Client ID of the user-assigned managed identity linked to your Azure resource.
***Client secret**	Enter your Azure client secret key.
***Credential name**	This field is displayed only when **Credential type** = **Credential List - CyberArk**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the CyberArk account with the Microsoft Azure credentials that will be used for onboarding the Azure account in AppViewX. The options listed in this dropdown list are the existing CyberArk accounts integrated with AppViewX. For instructions on integrating CyberArk with AppViewX, click here.
**: Mandatory fields*	

7. Enter/Select the details needed to **Discover Resources**.

Field description for the Discover Resources section

Field	Description
***Services**	From the dropdown list, select **Front Door** to map the service to the Azure setting.
***Subscription ID**	**Note:** This field is displayed only when **Account Type** = **Single Subscription**. Enter the unique identified (GUID) of your Azure subscription.
Auto Sync	To enable/disable automatic synchronization of the AppViewX inventory with your Azure cloud infrastructure , use the **Auto Sync** key. On enabling auto sync, the **Schedule Based** checkbox is displayed
Schedule Based	To specify a schedule for the auto sync: a. Click the icon. The **Schedule Based Sync** window is displayed. b. In the **General Information** section, enter the details of the sync schedule. For instructions, see Field descriptions for the General Information section.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the General Information section

Field	Description
***Frequency of Sync**	Set the sync frequency using the two dropdown lists for this field. For example, to set the frequency to 1 day: a. From the first dropdown list, select **1**. b. From the second dropdown list, select **Days**.
Advance Settings	To set the sync frequency for a specific service: a. Enable the **Advance Settings** key. The **Auto Sync Services** section is displayed. The services selected for this setting (in the **Services** field under **Discover Resources**) are listed in this section. b. To set the frequency for a specific service(s), select the corresponding checkbox. The **Service Specific Parameters** section is displayed with the **Frequency of Sync** field displayed for each selected service. c. Enter the details of the sync schedule and click **Apply**. The sync frequency is applied to the selected services. **Note:** If a service is not selected, the **Frequency of Sync** set in the **General Information** section is applied to all services in a setting.

8. From **Additional attributes**, for the **Front Door** service, select the user permission for **Cert sync** from the following options:
   - **Managed**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory. Users with the relevant permissions can then perform the required certificate-related actions.
   - **Monitored**: AppViewX will connect with the customer's Azure account and discover certificates. These certificates will be added to the inventory where the users will be allowed to only view the certificates.
   - **Ignored**: AppViewX will connect with the customer's Azure account but certificate discovery will be disabled.
9. Click **Save**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. Return to the **Device :: Cloud** page.
11. From the table of added devices displayed on the **Device :: Cloud** page, from the **Status** column, click **Check**.
    The status of the added device is displayed.
12. To view the certificates, go to (**Menu**) > **CERT+** > **CERTIFICATE INVENTORY** and select the required certificate type.

Onboarding Certificates for Microsoft Azure Devices in AppViewX

There are two ways you can onboard certificates in AppViewX:

- Via certificate discovery, for existing certificates
- Via certificate enrollment, for new certifcates

Discovering Certificates for Microsoft Azure Resources

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Cloud Scan**.
   The **Discovery : Cloud Scan : Add Discovery** page is displayed.
2. To initiate a cloud certificate discovery scan, enter/select the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	Cloud certificate discovery scan istriggered manually by the user as and when required.
Scheduled	Cloud certificate discovery scan is triggered automatically at the specified time and date.

   b. Enter/Select the details for **initiating an on-demand cloud certificate discovery scan**.

   Field descriptions for on-demand discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Note: Character limit: **2000 characters**

OR

Enter/Select the details for **initiating a scheduled cloud certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
Discovery Instance Name	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**. Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click **(Calendar** widget) to select a date to start the scheduled discovery.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget)
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. To filter the discovered certificates, enter/select the **Discover By** details.

Field descriptions for the Discover By section

Field	Description
***Discovery From**	From the dropdown list, select **Cloud** (the source to discover a certificate from).
***Vendor**	From the dropdown list, select **Azure**.
Discovery Scope	Select the Azure environment scope (range/boundary) within which the certificate discovery process will operate. • **Azure Settings** Azure settings are configurable parameters that define the behavior of the resources within a subscription. • **Azure Subscriptions** Azure subscriptions are logical containers that consitute the Azure services and resources, identified based on a customer's agreement with Microsoft.
Enable Service Specific Discovery	**Note:** This field is displayed only when **Discovery Scope** = **Azure Subscriptions**. To filter discovery results based on the services under each subscription mapped to a service, turn on the **Enable Service Specific Discovery** option.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If this field is disabled, the discovery scope will include all the services within a subscription that is mapped to a setting.
***Selected Resources**	To search for a resource: a. (Optional) In the **Type your search and press Enter** field, enter a search keyword to filter the list of resources. To make your search more specific: i. From the **Type your search and press Enter** field, click . ii. Enter/Select values for one or more of the following parameters: • **Azure Settings** • **Subscription ID** • **Tenant ID** • **Resource Type** iii. In the **Condition** field: • To get search results that meet all your specified criteria, select **AND**. • To get results that meet at least one (or more) of your specified criteria, select **OR**. b. From the search results, select the checkbox corresponding to the required resource. To add an existing resource to the list: a. Click . b. From the **Add Accounts** dialog box, select the checkbox corresponding to the required resource(s). c. Click **Add Selected**. **Note:** The **Add Selected** button is enabled after at least one resource is selected. To delete a resource from the list: a. Select the checkbox corresponding to the resource you want to delete. b. From the **Action** field, click .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	OR Click Remove. **Note:** To delete multiple resources at once: i. Select the checkboxes for the resources to be deleted. ii. Click Remove.
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter a interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered hee.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A setof filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter/select the following details:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select one from the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated. Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   Once the certificates are discovered, you can view them in the certificate inventory.

   To automate the certificate lifecycle management for the discovered certificates, you can enable auto regeneration of certificates, auto renewal of certificates, and auto push of certificates to endpoints.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enrolling Certificates

Enrolling a Server Certificate

Prerequisites

[For Linux-based vendor] OpenSSL is used to generate a private key and a Certificate Signing Request (CSR) as part of the endpoint enrollment process. Ensure that OpenSSL is installed and properly configured on the system before proceeding.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Renew Automatically**	**Note:** • If the Override feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA. From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request. To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})`

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. To generate the private key and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter the configuration details for CSR generation, refer the field descriptions given here.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. Enter the desired handler name in the field.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**. Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. In this field, enter the reference name assigned to the private key stored in/accessible to the selected ADC device.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • ADC • Cloud • Server • WAF • Firewall

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Run the following script to enable endpoint CSR generation support for **GlobalSignAtlas**: `db.getCollection('cert_metadata').insertOne({ "_id": "CSR_GENERATION_ENDPOINT_SUPPORTED_VENDOR_GLOBALSIGNATLAS", "objectMap": { "Server": [ "ABAP", "Web Dispatcher" ] } });` • On selecting GlobalSignAtlas CA, Category is automatically populated as Server.
Vendor	The dropdown list for this field is populated based on the **Category** selected. From the dropdown list, select the vendor for the end point device. **Note:** On selecting GlobalSignAtlas CA, Vendor is populated with ABAP and Web Dispatcher.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR. **Note:** On selecting **Vendor = Fortinet,** both Fortigate and FortiManager devices are populated. Auto-regeneration of certificates with FortiManager as endpoint is not supported.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Profile**	This field is applicable only when **Category** = **Server/WAF**. Select a profile from the dropdown list. **Note:** On selection of **Vendor = Imperva,** CSR generation at the endpoint is supported only for SaaS platforms. Profiles will not be displayed for AWS/on-prem deployments.
***Tenant**	This field is applicable only when **Category** = AD. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	This field is applicable only when **Category** = **Server**.
***Template Name**	This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** • As the extension is already included in the field, ensure that you enter the file name without the file extension. • Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter the vendor details.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Field descriptions for the CSR Parameters

Field	Description
Replace PSE File	The **Replace PSE File** checkbox enables users to generate the CSR or private key in the Server. This checkbox is displayed only in the case described below: a. Select the **CSR Generation** radio button as **Endpoint**. b. Select **Category** as *Server*, **Vendor** as *ABAP* or *Web Dispatcher* The Profiles dropdown is the only other field displayed below it and is populated with a list of .pse file names. c. Select the required **Profile** from the dropdown. Based on the values selected, the fields in the CSR Parameters section are auto-populated. The **Replace PSE File** checkbox is disabled by default and the SAN details fields in CSR Parameters section are also disabled. Selecting the checkbox will make the SAN details enabled and allow for values to be updated.
***Common Name**	Enter the certificate's common name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-). • For VMware vCenter, enter the device's FQDN to avoid certificates being rejected. If left blank, the FQDN will be auto-detected and populated.
Subject Alternative Name	From the dropdown list, select the **Subject Alternative Name** category for the certificate being enrolled. You can select more than one SAN category from the dropdown list. The cumulative count of SANs and the corresponding values are displayed in the certificate details (accessed from the holistic view in the certificate inventory). Depending on the SAN category selected from the dropdown list, corresponding fields are displayed for you to enter the required values.
DNS	Enter the domain names that the certificate will secure. Multiple domain names can be entered as a comma-separated list.
URI	This field is displayed when **Microsoft Enterprise** is the selected **Certificate Authority** and **URI** is one of the selected **Subject Alternative Name** categories. In this field, enter one or more URIs (URLs or URNs) that identify the resource(s) to be secured by the enrolled certificate. For a detailed description of URIs, URLs, and URNs, see the Glossary. **Examples of Valid/Correct URN** • urn:example:device123 • urn:ietf:rfc:8141 • urn:uuid:123e4567-e89b-12d3-a456-426614174000 • urn:org-id:org.acme:department42

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• urn:acme:product:router-x100:v1.2.3 • urn:example:svc+api-1.0@domain.com **Examples of Invalid/Incorrect URN** • urn::device (empty namespace) • URN:example:device (uppercase URN, **case-sensitive**) • urn:example: (empty NSS) **Important:** Ensure that the values entered here are in adherence to the CA policy enforcement type (strict or suggestive) selected for the Microsoft Enterprise CA.
Organization	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For VMWare vCenter, this is a mandatory field.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: For VMWare vCenter, this is a mandatory field.
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** • For renewal of the certificate being enrolled, country name is required. • For VMWare vCenter, this is a mandatory field.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate. **Note:** For VMWare vCenter, this is a mandatory field.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**. **Note:** The uploaded certificate validity for Globalsign MSSL is set to 365 days.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA. **Note:** • FortiManager supports only RSA key type of 512, 1024, 1536, 2048, 3072, 4096 bits. • VMWare supports only RSA of 2048, 3072, 4096, 7680, 8192 bits and EC key type.
***Bit Length**	From the dropdown list, select the required key size (in bits). The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you have uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.
   These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

   Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration. **Note:** The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the GlobalSign CA vendor specific details

Field	Description
For **Certificate Type** = **Alpha SSL**	
***Domain Admin Email**	From the dropdown list, select the email ID that will receive the approval requests from GlobalSign.
For **Certificate Type** = **Domain SSL**	
***Validation Type**	From the dropdown list, from the following options, select the DNS verification method that will be used by the CA to verify the domain challenge: • **DNS**: A specific DNS TXT record must be added to your domain's DNS configuration, either manually or automatically. The CA will query this DNS TXT record to verify the domain challenge. When **Validation Type** = **DNS**, the **Challenge Verify** dropdown list is displayed, allowing you to choose how the record will be added. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here. • **Email**: The CA will send a verification email to the selected domain contact. You must follow the instructions in the email to complete validation.
***Challenge Verify**	This field is displayed when **Validation Type** = **DNS**. From the dropdown list, from the following options, select the method for adding the DNS TXT record: • **Manual**: You must manually create the required DNS TXT record in your DNS configuration. For instructions, see Manually Verifying DNS TXT Records for GlobalSign Domain SSL Server Certificates. After the DNS TXT record is successfully validated and the certificate is issued, you can delete the DNS TXT record (optional).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Automatic**: AppViewX will automatically create the DNS TXT record using the configured DNS vendor and then request the CA to proceed with the validation. After the CA has successfully validated the DNS TXT record, it will proceed with certificate issuance. After the certificate is successfully issued, AppViewX will automatically delete the DNS TXT record. **Important:** For DNS validation, ensure that the **Enable DNS Automation** version of the **certificate_new_request** workflow is activated. Follow the workflow activation instructions given here.
***Vendor**	This field is displayed when **Challenge Verify** = **Automatic**. From the dropdown list, select the DNS vendor that supports automatic challenge verification. The current implementation of this feature supports the following two DNS vendors: **CloudFlare** and **Azure DNS**. **Note:** Ensure that the selected vendor is pre-integrated under the PKI category and supported by the system. For instructions on vendor integration, see the PKI+ Vendor Configurations documentation.
***Settings**	From the dropdown list, select the DNS vendor configuration setting that will be used by AppViewX to create, and later delete, the DNS TXT record. The options in the dropdown list are vendor settings pre-integrated in AppViewX. These settings enable AppViewX to programmatically create and remove DNS TXT records for the automatic challenge verification.
For **Certificate Type** = **Organization SSL**	
No additional vendor-specific details are required for this condition.	
For **Certificate Type** = **Extended SSL**	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Incorporating Agency Reg. No**	Enter the official registration number assigned to your organization by the government agency that authorized its incorporation. This number serves as a unique identifier for validating the legitimacy of an entity's legal existence and must match the records held by the relevant business registry.
***Designation**	Enter the designation of the requester.
***Business Category**	Enter the industry sector your organization operates in (for example, Information Technology, Finance, Healthcare, and so on). This gives GlobalSign a context of the nature of your organization and is used as part of the verification process.
**: Mandatory fields*	

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the Microsoft Enterprise CA vendor specific details

Field	Description
***Template Name**	From the dropdown list, select the template that will define the settings and policies for issuing the certificate from the Microsoft Enterprise CA. This list is populated based on the policy settings and group associations.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**. **Note:** • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Enrolling Client Certificates

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Client**
   The **Enroll Client Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter/Select the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	**Note:** Depending on the CA selected, the rest of the fields will be displayed. From the dropdown list, select the required certificate authority (CA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description

	Note: For enrolling certificates with policies using Google CA, consider the following points:
	
	Certificate Enrollment - Strict Policy
	• The Common Name will not be pre-filled from the policy.
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Certificate Enrollment - Suggestive Policy
	• The Common Name will not be pre-filled from the policy
	• The following validation will be seen based on strict policy guidelines.
	  • If the Common Name's domain name is not present in the **Allowed Domain Name** list, the non-compliant policy will be created.
	  • If the Common Name's domain name is present in the **Blocked Domain Name** list, an error validation will be shown upon saving the policy details.
	
	Note: For **Certificate Authority** = **EJBCA**, an additional set of fields, **Vendor specific details** is displayed after the **CA Details** section. Instructions on specifying the vendor specific details are covered in step 4.

***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120** **Note:** The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
Subscribe Email Alerts for Auto-Renewal	This field is displayed when **Renew Automatically** is enabled. To receive email notifications every time this certificate is auto-renewed, select this checkbox. The email notification includes certificate details, the type of auto action (renewal, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
Subscribe Email Alerts for Auto-Regenerate	This field is displayed when **Regenerate Automatically** is enabled. To receive email notifications every time this certificate is auto-regenerated, select this checkbox. The email notification includes certificate details, the type of auto action (regeneration, in this case), and the outcome (success/failure). These notifications help administrators stay informed of automated lifecycle actions, reducing the overhead to manually track them. If enabled here, this setting overrides the group setting for email alerts subscription, unless group-level overrides have been enforced.
***CA Account**	To which account the enrollment request to be submitted.
Certificate Type	Select the desired certificate type from the dropdown list.
***Division**	Select the division to which the certificate must be enrolled.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: This field will be shown only for Digicert CA.
Certificate Profile	**Note:** This field is applicable only for AppViewX CA and Google CA. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	Select the location of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuer Name**	Select the name of the issuer CA from the dropdown. **Note:** This is applicable only for Google CA.
***Issuance Policy**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the issuing policy for this certificate. An issuance policy defines the rules Futurex must follow to process the certificate enrollment request. The selected issuance policy will determine the

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	approval requirements for the certificate, the cryptographic settings, notification triggeres and other configuration parameters.
***Root CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the root CA for the certificate being enrolled. This is the trusted root certificate authority that anchors the certificate chain. All issued certificates will ultimately chain up to this root.
***Signing CA**	**Note:** This field is applicable only for Futurex. From the dropdown list, select the Certificate Authority that will sign the requested certificate.
***Extension Profiles**	**Note:** This field is applicable only for Futurex. Extension profiles enable you to further modify your certificates with additional field, attributes, and requirements. From the dropdown list, select the extension profile that will be used for the certificate being enrolled. To read more on and for instructions to create extension profiles, refer the Futurex documentation. For links, see the References section.
***Approval Group Name**	**Note:** This field is applicable only for Futurex. An approval group is a predefined set of users or roles authorized to approve the certificate enrollment request. From the dropdown list, select the approval group to authorize this enrollment request.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To read more on and for instructions to create and manage approval groups, refer the Futurex documentation. For links, see the References section.
***Connector Name**	Enter the friendly name for Certificate Authority connector in this field which will be displayed in the holistic view on saving this form.
Description	Enter the description in this field. **Note:** Character limit: **2000 characters**
***CSR Generation**	Select the CSR generation option as required. Options are: • **Upload CSR**: Uploaded CSR will be used as the source to populate CSR parameters and submit to CA. To upload a CSR: a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. On successful upload of this file, the CSR fields are populated with the corresponding details. • **HSM**: The private key and CSR will be created in the selected HSM device based on CSR parameters given. To generate the private key and the CSR, based on the CSR parameters given in an HSM device: a. Under **CSR Generation**, select **HSM**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **End Point**: The private key and CSR will be created in the selected end point device based on the CSR parameters given.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	To generate the private and the CSR, based on the CSR parameters given in an endpoint device: a. Under **CSR Generation**, select **End Point**. b. To enter/select the configuration details for CSR generation, refer the field descriptions given here. • **AppViewX** - Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` **Note:** For all CA types except Amazon, you have the option to generate the CSR.
**: Mandatory fields*	

Field descriptions for using HSM as the CSR generation source

Field	Description
***Device Type**	From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated: • **HSM Devices** (AppViewX will directly communicate with the HSM device for the CSR generation.) • **ADC Devices** (The selected ADC device will interact with the HSM to generate the CSR and subsequently transmit the relevant details to AppViewX.)
***Vendors**	This field is displayed only when **Device Type** = **ADC Devices**. From the dropdown list, select the required ADC device vendor.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Module Number	This field is displayed when **Device Type** = **ADC Devices** and **Vendors** = **Thales**. In the event that multiple HSMs are configured on a system, module number is a unique identifier assigned to each HSM. In this field, enter the module number assigned to the selected Thales device.
***Devices**	From the dropdown list, select the required HSM/ADC device. This field is populated based on the **Device Type** and **Vendors** selected. • For **Device Type** = **HSM Devices** The dropdown list is populated with HSM devices that were enabled for CSR generation at the time of onboarding and have been successfully onboarded. To read more on onboarding HSM devices in AppViewX, click here. • For **Device Type** = **ADC Devices** The dropdown list is populated with F5 devices that are in the **Managed** state. Currently, AppViewX enables HSM key generation only through F5 devices for the following HSM vendors and their respective supported versions: • Fortanix (v14 and onwards) • Thales (v12 and onwards) • Safenet (v12 and onwards)
***Key Handler Name**	This field is displayed when **Device Type** = **HSM Devices**. Key handler name refers to an identifier used to reference a cryptographic key managed by an HSM device. In this field, enter the reference name assigned to the Master Encryption Key stored in the selected HSM device.
***Key Reference Name**	This field is displayed when **Device Type** = **ADC Devices**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Key reference name refers to an identifier used to reference a private key that is stored locally on an ADC device or is securely accessible to the device via an external HSM. Enter the desired handler name in the field.

Field descriptions for using an endpoint device as the CSR generation source

Field	Description
Category	From the following options, select the ADC device category: • **ADC** • **Cloud** • **Server** • **Firewall**.
Vendor	From the dropdown list, select the vendor for the end point device. **Note:** The dropdown list for this field is populated based on the **Category** selected.
***Devices**	This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.
Tenant	**Note:** This field is applicable only when **Category** = **ADC**. Enter the tenant ID.
***Service name**	From the dropdown list, select the cloud service running on the selected cloud **Devices**.
CSR Location	**Note:** This field is applicable only when **Category** = **Server**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Template Name**	**Note:** This field is applicable only when **Category = Firewall**. Select the required template from the dropdown list. **Note:** • This field will be enabled when the Platform = Panorama while onboading PaloAlto device at **Menu** > **CERT+** > **Device Management** > **Inventory**> **Firewall** > **Add**. • Templates and partitions are used to enroll certificates at the template level. To enroll a certificate at the **Panorama** level, set the template to **None**.
Partition	**Note:** This field is applicable only when **Category** = **Firewall**.
***CSR File Name**	Enter the name of the file that contains the CSR parameters. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension. **Note:** Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **CSR File Location**.
***Key File Name**	Enter the name of the file that contains the private key details. **Note:** Since the extension is already included in the field, ensure that you enter the file name without the file extension.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: Starting v2023.1.0 FP2, for enrolling Apache server certificates, this field is labeled as **Key File Location**.
***Certificate File Name**	**Note:** This field is displayed only when **Category** = **Cloud**. Enter the certificate file name.
***Key vault**	**Note:** This field is displayed only when **Category** = **Cloud**, **Vendor** = **Azure**, and **Service name** = **Key Vault (Azure)**.
***Service**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. This dropdown list is populated based on the **Device** selected. From the options in the dropdown list, select the service.
***Exchange Server**	**Note:** This field is displayed when **Category** = **Server** and **Vendor** = **Microsoft Server**. From the dropdown list, select the name of the MS Exchange server for which the certificate is being enrolled.

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
**: Mandatory fields*	

5. Enter/Select the **CSR Parameters**.

Field descriptions for the CSR Parameters section

Field	Description
***Common Name**	The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, <appviewx>. No special characters allowed except en dash (_) and hyphen (-).
***Common Name Indicator**	**Important:** See note. This field is displayed when the selected **CA Account** is **DigiCert** and **Certificate Type** is one of the following: • Secure Email for Business • Digital Signature • Premium As part of DigiCert's revised security regulations, the common name for the above listed DigiCert certificate types is derived from the one of the input attributes, as selected from the dropdown list. For the common name indicator, from the dropdown list, select one of the following: • **First Name and Last Name** • **Pseudonym** • **Email** (applicable only for the **Secure Email for Business** certificate type)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***First Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified first name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.
***Last Name**	This field is displayed when: • **Common Name Indicator** = **First Name and Last Name** • **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** Enter the verified last name of the individual subject. For **Common Name Indicator** = **First Name and Last Name** A combination of the first name and last name will be used to derive the certificate's common name, which will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from the holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **First Name and Last Name** The first and last name will be appended as mandatory additional information to the Subject Alternative Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Pseudonym**	This field is displayed when: • **Common Name Indicator** = **Pseudonym** • **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** Enter the pseudonym of the individual subject. A pseudonym is a fictitious name assumed for a particular person. For **Common Name Indicator** = **Pseudonym** The entered pseudonym will be displayed in the certificate's **Common Name** field or the **Subject DN** (in the certificate details that can be accessed from trhe holistic view). For **Common Name Indicator** = **Email** and **Indicator Type** = **Pseudonym** The pseudonym will be appended as mandatory additional information to the Subject Alternative Name.
***Indicator Type**	This field is displayed when **Certificate Type** = **Secure Email for Business** and **Common Name Indicator** = **Email**. In this case, the issuer's email address, as specified in the CSR parameters, is used to derive the common name. For **Common Name Indicator** = **Email**, it is mandatory to include additional information in the form of the first name and last name or the pseudonym, which will be appended to the Subject Alternative Name. From the following options, select the required indicator type to be used as mandatory information along with the email: • **First Name and Last Name** The **First Name** and **Last Name** fields are displayed. • **Pseudonym** The **Pseudonym** field is displayed.
Subject Alternative Name	You can see the count of subject alternative names (SAN) available for a certificate in the CSR parameter section, inventory grid, and CA connector page.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Select the subject alternative subject name from the dropdown list. The possible options are, • Select all • DNS • IP Address. **Note:** • Multiple values must be separated by a comma. • The cumulative count SANs appears in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Country**	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on).
Email Address	The email contact details of the person responsible for maintaining the certificate. Enter the valid e-mail address.
***Order Validity**	Enter the number in this field and select the entered validity list to be in Days, Months, and Years from the dropdown list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The **Order Validity** for the following DigiCert S/MIME certificate types cannot exceed **2** years: • Secure Email for Business • Digital Signature • Premium **Note:** As per revised security regulations for DigiCert S/MIME certificates, the maximum lifespan of the the above listed certificate types is **two** years.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Reenter the same password to confirm that is entered in the Challenge Password field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).
***Key Type**	From the dropdown list, select the cryptogrpahic algorithm that will be used for generating the certificate's key pair. The dropdown list is populated based on the CA policy configured for the selected CA.
***Bit Length**	From the dropdown list, select the required key size (in bits).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	The dropdown list is populated based on the CA policy configured for the selected CA.
***ECDSA curve**	For **Key Type** = **EC**, from the dropdown list, select the elliptic curve that will be used to create the public and private key pairs.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter the alternate name for the document to be uploaded.
Comments	Enter the comments in this field. **Note:** Character limit: **2000 characters**
Upload File	Click the Upload button to select the file.

7. Other than the CSR fields, you can add organization-specific values along with CSR. These values will not be part of the certificate but will be available in the AppViewX inventory. For example, cost center. Inventory can be filtered based on these attributes as well. In the Certificate Attributes can be added under Administration > certificate attributes, it will be reflected on the enrollment page:
8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit logentries (typically enrollment and revocation events)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Certificate holder Email	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Last name (as a metadata) associated with the certificate to be enrolled
Organization	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** For the IDnomic CA, this field is displayed only when the selected CA account has been configured using a Registration Authority (RA). Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	• **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

> **Note:** If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is completed, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

    If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

    If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

    Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Pushing Certificates to Microsoft Azure Front Door

> **Important:** Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Azure Front Door

1. To create an application connector for pushing a certificate, go the holistic view of the certificate.
   To do this:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. Go to (**Menu**) > **CERT+** > **Certificate Inventory** and select the required certificate category.

b. From the certificate inventory displayed, select the **Common Name** of the certificate you want to push.
The holistic view of the certificate is displayed.

2. On the certificate holistic view, click **Add Connector**.

3. Enter/Select the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Cloud**.
***Vendor**	From the dropdown list, select **Azure**.
Service Types	From the dropdown list, select **Front Door**.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available Microsoft Azure Front Door profiles and domains already onboarded in AppViewX.

You can push a certificate to a profile (and therefore to all domains within that profile) or to selected domains within a profile.

4. To select the profile(s)/domain(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, for the required profile(s)/domain(s), click .
The **Selected devices** list is updated according to your selection.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

5. Enter/Select the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
***Secret Name**	This field is displayed when **Service Type** = **Front Door**. Enter the name of the secret in Azure Key Vault that stores the certificate to be pushed to Azure Front Door.
***Key Vault Subscription ID**	This field is displayed when **Service Type** = **Front Door**. Enter (a new)/Select (from an existing list) the Azure subscription ID for the Key Vault from which the certificate is to be retrieved.
***Key Vault Name**	This field is displayed when **Service Type** = **Front Door**. From the dropdown list, select the name of the Key Vault in which the certificate is stored.
Replace Certificate in Key Vault	This field is displayed when **Service Type** = **Front Door**. Use the toggle key to specify whether an existing certificate in the specified Key Vault should be overwritten with the new one during the push operation.
***Key Vault Certificate Name**	This field is displayed when **Service Type** = **Front Door**. Enter the logical name under which the certificate is stored in the Key Vault.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificate, select this checkbox.

6. Enter/Select the **Push Details**.

Field descriptions for the Push Details

Field	Description
Pre - Push Script File Name	Enter the file name of the pre-push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

7. Click **Save**.
   The connector is displayed on the certificate holistic view.

Pushing a Server Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

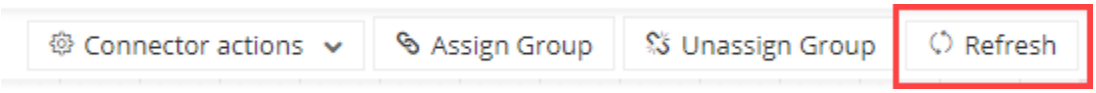
- The approval process is triggered. The current flow is based on the default policy of two-level approvals.
- A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Pushing a Client Certificate

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Client**.
   The **Client Certificate** page is displayed.
2. To push a certificate, under **Common Name**, double click the required certificate.
   The certificate topology view is displayed.
3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- The approval process is triggered. The current flow is based on the default policy of two-level approvals.
- A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.

6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

   d. Click **Update**.

2. To enable auto push for the certificate connector:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
   To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
   The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
   The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

References

- Create an Azure Front Door Profile using the Azure Portal.
- Configure managed identities on Azure virtual machines.

Automating CLM for Microsoft SQL

Prerequisites

- **Access Requirements:**

  To perform certificate management operations, the user managed in **AppViewX** must have the following permissions:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

  - **Read and write access to the trust store** (to discover and push certificates).
  - **Read and write access to the Windows registry** (to update certificate thumbprints and enforce encryption settings).
- Ensure that PowerShell and WinRM tools are installed and running on the Windows machine.
- Verify that Microsoft SQL instance are available and running on the Windows machine.
- (Optional) If the Gateway type is selected as WMI, ensure that WMI is properly configured.
- If the SQL Server instance is running under a service account that is neither Local System nor a member of the Administrators group:
  - **For a Domain Service Account**: Add the account to the Administrators group on the server.
  - **For a Built-in Account (for example, Network Service)**: If the service account cannot be added to the Administrators group, use the Default connector to push the certificate. For the post-script execution, refer to Certificate Post script execution approach to Bind Certificates.
    - You can then leverage post-script execution to:
      - Grant read access to the certificate's private key.
      - Perform the bind operation.

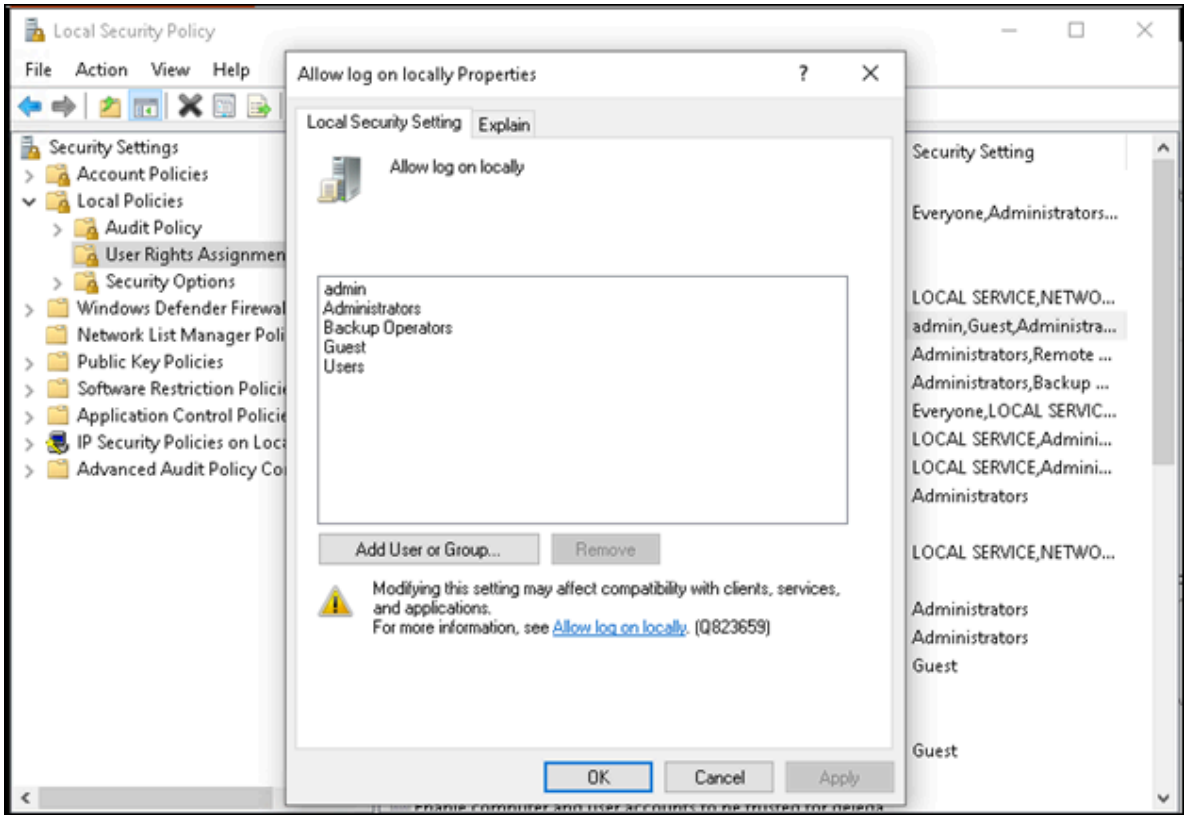
Prerequisites for Managing Windows Servers Using PowerShell Mode

To successfully manage **Windows servers** in **PowerShell mode**, ensure the following prerequisites are met.

1. Local Administrator Account on Target Machines.
   a. The **account used for onboarding** the device must be a member of the **Local Administrators Group** on the target machine.
   b. This account is required for **device onboarding** and **enabling remote PowerShell sessions**, as administrative privileges are essential for remote management.

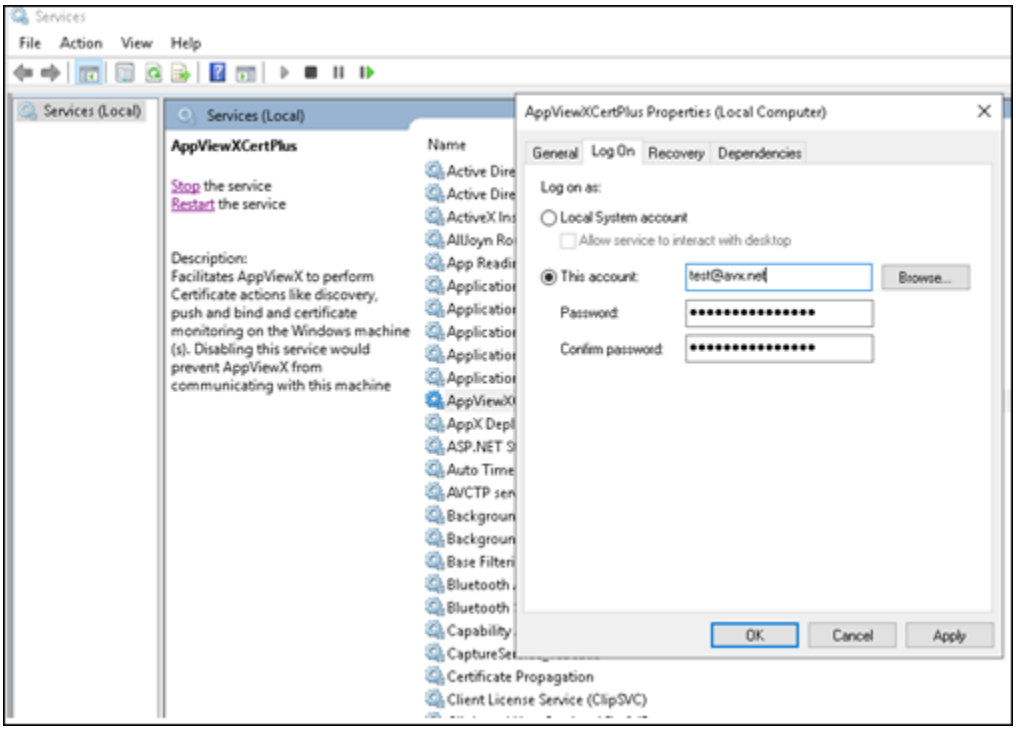
Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: If the onboarding account is **not** a **Local Administrator** on the Windows agent machine, it must be granted **Allow Logon** rights in the machine's policies.



2. Logon Service Account on the Windows Agent Machine: The Windows agent machine must have a logon service account with local administrator privileges to run the required services.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



3. Network Ports.

   To enable seamless communication between the **target machines**, the **Windows agent machine**, and the **Cloud Connector (CC)**, ensure the following ports are open:

   - Port 5985 (WSMAN) – Required on both the **target machines** and the **Windows agent machine** for **remote PowerShell functionality**.
   - Port 445 (SMB) – Needed for **certificate transfer** to the target machines using the **SMB protocol**.
   - Port 8999 – Must be open on the **Windows agent machine** to facilitate communication with the **Cloud Connector (CC) or AppViewX (AVX)**.

4. Check Connectivity from CC to Gateway.
   a. Login to **AppViewX** pods CLI to check communication.
      i. **On Prem :** Login in **AppViewX** CLI, go to vendor pods.
      ii. **Saas :** Login to CC, platform pod.
   b. After logging in run the below commands in terminal.

```
nc -zv <Ip or hostname> <8999 or configured port>
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

> **Note:**
> - The <IP or hostname> refers to the **hostname** or **IP address** of the **Windows agent machine**.
> - **Port 8999** is the **default port** for the **Windows Agent**. *(If a custom port is configured, use the specified port instead.)*

- **Expected Output:**

```
Connection to 192.xxx.142.xx 8999 port [tcp/*] succeeded!
```

5. Check Connectivity from Windows Gateway Machine to Target Machine: Run the following command in Windows PowerShell, replacing <port> and <hostname> with the actual values of the Windows agent and target machine:

```
Test-NetConnection -ComputerName <hostname> -Port <port>
```

- Output Example:

```
ComputerName : computername
RemoteAddress : 93.184.xxx.xx
RemotePort : 80
InterfaceAlias : Ethernet
SourceAddress : 192.168.x.xx
PingSucceeded : True
TcpTestSucceeded : True
```

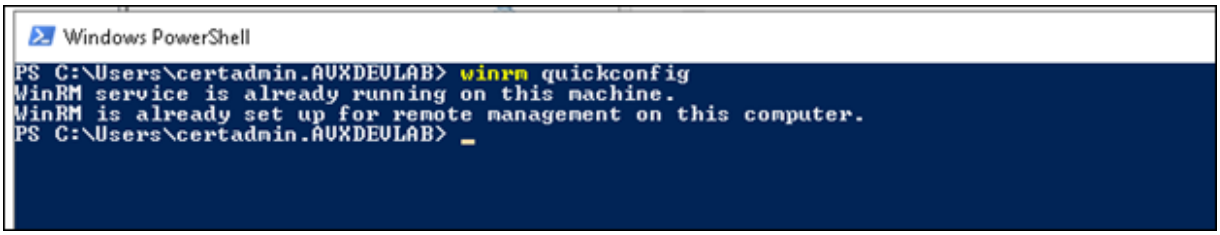
6. Check Remote Powershell Session from Windows Gateway Machine to Target Machine: Open an administrator powershell and run the following command from the Windows Gateway Machine to the target machine.

```
Enter-PSSession -computerName <hostname> -credential <username>
```

> **Note:**
> - <hostname>: Add the hostname of the remote machine.
> - <username> : Username of the service account.
> - For troubleshooting WinRM related errors, refer to PowerShell to a Remote Server via WinRM.

7. Ensure that Remote powershell is enabled in the target machines.Test using ***winrm quickconfig*** .

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



8. Kerberos Authentication.
   - Ensure all accounts are within the **same domain** to enable **Kerberos authentication** for remote PowerShell connections.
   - Validate the **Kerberos setup** between the **target machines** and the **Windows agent machine** to ensure proper **authentication and communication**.

Prerequisites for Windows Gateway and Target Server Configuration

Requirement	AppViewX Windows Gateway	Target Server
User account type	Service account with local admin	Service account with local admin
Services	RPC Service WinRM Service WinRM Configuration Powershell remoting certutil.exe command availability	RPC Service WinRM Service WinRM Configuration Powershell remoting certutil.exe command availability
Ports	8999(Customisable) 5985 - WSMAN 445 - SMB: Required only for certificate push functionality.	5985 - WSMAN: Enables remote PowerShell functionality. 445 - SMB: Required only for certificate push functionality.

Onboarding Microsoft SQL Server

1. Go to (**Menu**) > **CERT+** > **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click the **(Add)** icon.
   The **Device details** page is displayed.
4. Select **Microsoft SQL** from the Vendors list.
5. In the **Server details** section, select/enter the details as follows.

Server Details - Field Description Table

Fields	Description
***Server name**	Enter the name of the designated Microsoft SQL server.
Communication mode	Select the Gateway or SSM protocol to be used for communication between the AppViewX node and the Microsoft SQL Server.
***Hostname**	Enter the hostname of the Microsoft SQL server.
Data center	Choose the desired datacenter. The communication to the device will be routed to through this datacenter from AppViewX and the communication will be routed to this datacenter alone when strict routing is enabled.
Cert Sync	Choose from the any of the following: • *Managed* - AppViewX performs the config fetch operations and the certificates are discovered and managed in the inventory. CLM actions (push & bind, rollback etc.) can be performed on them. • *Monitored* - AppViewX performs the config fetch operations and the certificates are downloaded in the inventory in the read-only state. CLM actions cannot be performed on them. • *Ignored* - AppViewX only performs the config fetch operations for the devices. There is no certificate discovery performed.
**: Mandatory fields*	

6. In the **Credentials** section, select/enter the details as indicated below. The credentials entered in this section are used to authenticate the session between the AppViewX node and the Microsoft SQL device.
   If **Communication mode** = **Gateway** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - AppViewX

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: The dropdown displays the credential types configured in the Device Credential section. Additionally, AppViewX supports the following external credential types: • HashiCorp • CyberArk • BeyondTrust • Thycotic.
***Username**	Enter the designated username for authentication. **Note:** This field is displayed only if the credential type is selected as **Manual Entry**.
***Password**	Enter the secure password. **Note:** This field is displayed only if the credential type is selected as **Manual Entry**.
**: Mandatory fields*	

If **Communication mode** = **SSM** the fields are as follows:

Credentials - Field Description Table

Fields	Description
***Credential Type**	Select the credential type from the dropdown. • *Manual entry* (default) • *Credential List* - cloudAccount **Note:** If **Credential list - cloudAccount** is selected, the ***Account name** dropdown field is displayed. Select any of the preconfigured credential values.
***Access key**	Enter the access key to login to the EC2 instance of the AWS cloud machine.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Secret key**	Enter the secret key to login to the EC2 instance of the AWS cloud machine.
**: Mandatory fields*	

7. Enter/Select the **Windows gateway details**.

> **Note:** This section is displayed only when **Communication mode** = **Gateway**.

Windows Gateway Details - Field Description Table

Fields	Description
***Windows Gateway Mode**	**Note: Applicable only for SAAS**. For communicating with Windows-based devices, from the following options, select the gateway agent mode to be used: • **External** This mode will use the AppViewX Windows Gateway Agent that is set up on a Windows device. • **Integrated** Tech Preview This mode will use the prepackaged gateway that is integrated in the AppViewX Cloud Connector (**enabled only in the SaaS and Managed Kubernetes installations**). Prerequisites for using the Integrated Windows Gateway mode

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
	Note: This is only a tech preview, which means the feature is under development. The tech preview has been released for testing and evaluation by the general audience. Necessary improvements will be made before the official release. Currently, this feature is not recommended for production. **Note:** The integrated gateway functionality is not compatible with the following features: • Server addition using the **import** feature • Endpoint CSR generation
***Gateway type**	**Note: Applicable only for SAAS**. From the following options, select the required gateway type: • PowerShell • WMI. **Note:** The integrated gateway uses only the PowerShell gateway command execution mode and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.
***Gateway location**	From the following options, select the gateway location: • **Remote** **Note:** By default, the integrated gateway is remotely located. and therefore, this field is not displayed when **Windows Gateway Mode** = **Integrated**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Fields	Description
***Select gateway**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External**. From the following options, select the gateway: • **New** • **Existing**.
***Windows gateway**	**Note:** This field is displayed only when **Select gateway** = **Existing**. From the dropdown list, select an existing Windows gateway.
***Windows gateway name**	For **Windows Gateway Mode** = **External** and **Select gateway** = **New**, enter a name for the Windows Gateway. For **Windows Gateway Mode** = **Integrated**, this field is auto-populated with the value **integrated-gateway**.
***Windows gateway URL**	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Enter the URL of the Windows Gateway endpoint.
Client authentication certificate	**Note:** This field is displayed only when **Windows Gateway Mode** = **External** and **Select gateway** = **New**. Upload the client certificate used while installing Windows Gateway. You can use the default client certificate (**ClientCertificateGateway.pfx**) or a custom certificate.
**: Mandatory fields*	

8. Enter/Select the **Vendor Specific Details**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note: This section is displayed only when **Communication mode** = **SSM**.

Vendor Specific Details - Field Description Table

Fields	Description
***Region**	Enter the geographic region of the AWS instance. *Example*: us-east-2
***Instance Id**	Enter the unique identifier for an EC2 instance in AWS. It is required to perform actions or execute commands on a specific EC2 instance *Example*: i-02573cafcftext **Note:** Click the (**Settings**) icon next to the field to configure the ARN Advanced Settings.
***SSM document name**	Enter the name of the SSM document that contains the script or action to be executed on the EC2 instance. *Example*: **AWS-RunShellScript** is an SSM document that allows you to execute shell scripts on EC2 instances.
***SSM document version**	Specify the version of the SSM document to be executed. *Example*: 1
***S3 bucket name**	Enter the S3 bucket name used to store command output or logs executed in the EC2 instance. *Example*: avxdiscoverydocument-c2 **Note:** Click the (**Settings**) icon next to the field to configure the S3 Advanced Settings.
Proxy Required	Select the checkbox to enable the secure proxy service.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

9. Click **Save**.
   The device is onboarded successfully.

Validating the Device

After the device is onboarded successfully, follow the steps to validate the device communication with AppViewX:

1. Go to **ADMINISTRATION** > **Device Management**.
   By default, the **ADC** tab opens.
2. Click the **Server** tab.
   The Server Inventory page is displayed.
3. Check that the device name appears in the inventory (Name column) with the specified CertSync status (Status Column).
   The status column will have the value Managed/Monitored/Ignored based on the CertSync status if the connection is successful or displays Failed/Unresolved in case of failure.
4. From the Status column, click the Managed/Monitored.
   Device Status Log pop-up is displayed.
5. Expand each value in the pop-up to know the **Device communication**, **Device Version**, **Instance Information**, and **Certificate Discovery From Device**.

Discovering Certificates for Microsoft SQL

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE DISCOVERY** > **Discovery** > **Managed Devices Scan**.
   The **Discovery : Managed Devices Scan : Add Discovery** page is displayed.
2. To initiate a managed devices scan, enter the **Discover Details**.

   a. To specify the frequency at which the certificate discovery scan will be triggered, select the **Discovery Run Type**.

   Discovery run type options

Frequency Type	Description
On-demand	The certificate discovery scan will be triggered manually by the user as and when required.
Scheduled	The certificate discovery scan will be triggered automatically at the specified time and date.

   b. Enter the details for **initiating an on-demand managed devices certificate discovery scan**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for on-demand discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**

OR

Enter the details for **initiating a scheduled managed devices certificate discovery scan**.

Field descriptions for scheduled discovery

Frequency Type	Description
***Discovery Instance Name**	Enter a name for the discovery instance.
Description	Enter additional details related to the discovery option. **Note:** Character limit: **2000 characters**
Time Zone	Select your time zone.
Occurrence Type	From the dropdown list, from the following options, select an occurrence frequency: • **Daily** • **Weekly** • **Monthly** • **Yearly**
***Repeat On**	**Note:** This field is displayed only when **Occurrence Type** = **Weekly**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Frequency Type	Description
	Select the checkbox corresponding to the day of the week on which you want the discovery occurrence to repeat.
***Starts On**	Click (**Calendar** widget) to select a date to start the scheduled discovery.
***Ends**	From the following options, select when the scheduled discovery is to end: • **Never**: Discovery never stops. • **After**: Discovery stops after the number of occurrences specified in the text field. • **On**: Discovery stops on the date selected using **(Calendar** widget).
Summary	Displays a summary of the selections made for scheduled discovery
**: Mandatory fields*	

3. In the **Discover By** section, enter the discovery details.

Instruction for discovering certificates

Field	Description
***Discovery From**	From the dropdown list, select **Managed Servers**.
Devices window	A list of all the managed server devices is displayed in the devices window. To select devices for certificate discovery, select the checkbox(es) for the required devices. The devices window has the following option: • **Search**: Enter keywords to filter and select the desired vendor or device name from thematching results. • **Add as Favorites**: You can mark your frequently used devices as favorites. • **All**: Select this to see the complete list of devices (unfiltered). • **Selected**: Select this to list only the selected devices. • **Unselected**: Select this to list only the unselected devices. • **Delete**: Delete the required devices from the favorites list.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Execute Batches Sequentially	To execute the discovery operation on the specified batches sequentially, select this checkbox.
***Interval Between Batches**	If **Execute Batches Sequentially** is selected, enter an interval duration (in minutes) in this field. The sequential execution of the batches is spaced according to the interval value entered here.
***Discovery Type**	From the following options, select one: • **All Certificates**: Select this to discover all certificates. • **Certificates in Use**: Select this to discover only those certificates that are associated with a service.
**: Mandatory fields*	

4. In the **Discovery Rules** section, from the **Associate Rule** dropdown list, select a rule that will be used to filter the discovered certificates.
   A set of filters is combined to create a rule, from the **Rules** menu. The selection of rules will apply respective filters on discovered certificates.
5. In the **After Discover** section, enter the following details:

Field descriptions for the After Discover section

Field	Description
***Move Certificate to Inventory with Status**	Select from one of the following options: • **Do not move**: The newly discovered certificates and their objects will not be moved to the inventory. • **Managed**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Managed**. • **Monitored**: The newly discovered certificates and their objects will be moved to the inventory with the status set to **Monitored**.
Use Access Control Rule	To apply the rule configured using Access Control, select this checkbox. **Note:** If this checkbox is enabled, the certificate group will be associated automatically by the rule in access control.
***Certificate Group**	From the dropdown list, select a certificate group to which the discovered certificates will be associated.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Based on the group association, a policy will also be applied to these certificates, which will help ascertain compliance or non-compliance.
**: Mandatory fields*	

6. Click **Discover**/**Schedule** to trigger the on-demand/scheduled discovery, respectively.
   The discovered certificates are displayed in the certificate inventory.
7. AppViewX follows these steps to retrieve the appropriate server certificate.

   a. Identify the certificate thumbprint currently bound in the Windows registry.

   b. Retrieve all certificates from the local trust store.

   c. Match the retrieved certificates against the stored thumbprint to determine the active server certificate.

   AppViewX automatically detects all SQL instances running on the target Microsoft SQL Server machine and creates individual profile connectors for each instance. These connectors enable certificate push and binding operations specific to each SQL instance.

8. Each profile connector is named using the following convention:

   a. <hostName>:<instance>

   > **Note:** This format ensures the unique identification of each SQL Server instance.

   b. In addition, AppViewX automatically creates a **default connector**, which supports only the certificate push operation.

Enrolling a Server Certificate

Server certificate enrollment refers to the process of creating a digital ID for an application/web server hosted in the network. It starts with the generation of a key pair (private and public key) and CSR, and then submitting the CSR to the required CA to procure a certificate. CERT+ supports the generation of keypair on the device, HSM, AppViewX. Users can also upload the CSR for enrolling for a digital certificate.

To enroll a server certificate:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Enroll Certificate** > **Server**
   The **Enroll Server Certificate** page is displayed.
2. In the **General Information** section, from the dropdown list, select the required **Assign Group**.
3. Enter the **CA Details**.

Field descriptions for the CA Details section

Field	Description
***Certificate Authority**	From the dropdown list, select the certificate authority to request the certificate enrollment. **Note:** The IDnomic CA can be used for issuing certificates only in an on-prem deployment. Certificates issued through IDnomic CA can be renewed only if they are enrolled using a Registration Authority workflow.
***Renew Automatically**	**Note:** • If the **Override** feature is enabled for the certificate group selected from the **Assign Group** dropdown list, auto renew settings done in the enrollment page will be overwritten by the group level settings. • If **Regenerate Automatically** has been enabled for the selected certificate group, the **Renew Automatically** field is not displayed here. To automatically renew this certificate: a. Turn on the **Renew Automatically** toggle. The ***Start Renewing** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the renewal process should start. Valid range for number of days: **1** to **120**

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The auto renew settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was renewed manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
***Regenerate Automatically**	To automatically regenerate this certificate: a. Turn on the **Regenerate Automatically** toggle. The ***Start Regenerating** field is displayed. b. In the **Days Before Expiry** field, specify how many days prior to a certificate's expiry the regeneration process should start. Valid range for number of days: **1** to **120** **Note:** This value can exceed the certificate's validity in case of short-lived certificates. **Note:** • This feature can be enabled only for valid certificates (not for revoked/suspended and expired certificates). • The auto regenerate settings from the parent certificate will be transferred to the child certificate only if the toggle was enabled; they will not transfer if the certificate was regenerated manually. After migration, these settings will be disabled for the parent certificate, so enable them manually if needed.
***CA Account**	From the dropdown list, select the CA account to which the certificate enrollment request will be submitted.
Certificate Type	From the dropdown list, select the required certificate type.
***Division**	**Note:** This field is applicable only for Digicert CA.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	From the dropdown list, select the division with which the certificate will be enrolled.
Certificate Profile	**Note:** This field is displayed for only selected CAs. For the IDnomic CA, this field is displayed when only-CA setting is selected from the **CA Account** dropdown list. From the dropdown list, select the certificate profile with which the certificate must enroll.
***RA Workflow**	**Note:** This field is displayed when **Certificate Authority** = **IDnomic** and a CA+RA setting is selected from the **CA Accounts** dropdown list. From the dropdown list, select the RA workflow that will be used for certificate enrollment. For the details of a workflow, you can check them on your CA portal on IDnomic.
***Issuer Location**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer location associated with the CA account.
***Issuer Name**	**Note:** This field is applicable only for Google CA. From the dropdown list, select the issuer name for issuing the certificate.
***Connector Name**	Enter a friendly name for the CA connector. On saving this form, the name entered here will be displayed in the holistic view.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Description	**Note:** Character limit: **2000 characters** Enter the description in this field.
***CSR Generation**	**Note:** This field is applicable for all CAs **except Amazon**. From the following options, select the required method for generating the CSR: • **AppViewX**: Private key and CSR will be created in AppViewX based on CSR parameters given. **Note:** If auto regeneration has been enabled for this cerificate, AppViewX can be enforced as the default CSR generation source (irrespective of any selections made here) every time the certificate is regenerated. To do this, execute the following db script: `db.cert_metadata.insertOne({"_id":"CERT_AUTO_REGENERATE_DEFAULT_APPVIEWX_CSR", "flag":true})` • **Upload CSR**: You can upload a file that contains the CSR details. This source file will be used to populate the CSR parameters, which will then be submitted to the CA. a. Under **CSR Generation**, select **Upload CSR**. The **Please paste your CSR** field is displayed. b. From the **Please paste your CSR** field, select **Browse**. c. Navigate to the location of your CSR file, and click **Open**. d. Click **Upload**. • **HSM**: **Note:** This option is disabled/not displayed when **Certificate Authority** = **Google**, **CSC Global**, and **DigiCert One**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>To generate the private key and the CSR, based on the CSR parameters given, in an HSM device:
a. Under CSR Generation, select HSM.
b. Fields for gathering your HSM-related inputs are displayed.
To generate the private key and the CSR, enter/select the following details:
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>*Device Type</td><td>From the dropdown list, from the following options, select the type of device on which the private key and the CSR will be generated:
• HSM Devices
• ADC Devices</td></tr>
<tr><td>*Vendors</td><td>Note: This field is applicable only when Device Type = ADC Devices.</td></tr>
<tr><td>*Devices</td><td>From the dropdown list, select the required HSM/ ADC device.
Note: This field is populated based on the Device Type and Vendors selected.</td></tr>
<tr><td>*Key Handler Name</td><td>Note: This field is applicable only when Device Type = HSM Devices.
Enter the key handler name.</td></tr>
</table></td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>***Key Reference Name**</td><td>**Note:** This field is applicable only when **Device Type** = **ADC Devices**. Enter the key reference name.</td></tr></table> • **End Point**: **Note:** This option is disabled when **Certificate Authority** = **Google** and **CSC Global**. **To generate the private key and the CSR in the selected end point device, enter the following inputs:** <table><tr><th>Field</th><th>Description</th></tr><tr><td>**Category**</td><td>From the following options, select the **Server** device category from the dropdown list.</td></tr><tr><td>**Vendor**</td><td>From the dropdown list, select the MS SQL vendor for the end point device from the dropdown list. **Note:** The dropdown list for this field is populated based on the **Category** selected.</td></tr><tr><td>***Devices**</td><td>This field lists the end point devices present in your environment that belong to the above selected **Category** and **Vendor**. From the dropdown list, select the end point device on which you want to generate the private key and the CSR.</td></tr><tr><td>***CSR File Location**</td><td>Enter the valid CSR file location. For example, C:\filepath\filename.</td></tr></table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>Note: This field is applicable only when Category = Server.</td></tr>
<tr><td>*Key File Location</td><td>Enter the valid key file location. For example, C:\filepath\filename.

Note: This field is applicable only when Category = Server.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">*: Mandatory fields</td></tr>
</table>

4. For the **EJBCA** certificate authority, enter/select the vendor details.

Field descriptions for the EJBCA Vendor Specific Details section

Field	Description
* **End Entity Profile Name**	From the dropdown list, select the end entity profile name.
End entity user name	Enter the name of the end user entity.
* **Issuer Common Name**	From the dropdown list, select the issuer common name.
***Certificate Profile Name**	From the dropdown list, select the certificate profile name.
*: Mandatory fields	

5. For the certificate being enrolled, enter the **CSR Parameters**.

Note: For DigiCert One, all CSR parameters that are assigned static values in the certificate profile will be auto-populated and disabled for editing.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSR Parameters

Field	Description
***Common Name**	Enter the certificate's common name. The common name is one of the key values of Certificate Signing Request (CSR) to be present in the certificate. For example, **<appviewx>**. **Note: Constraints**: • Character limit: 64 characters • No special characters allowed except en dash (_) and hyphen (-).
Subject Alternative Name	From the dropdown list, select the Subject Alternative Name category for the certificate being enrolled. In the corresponding field(s) displayed for the selection made, enter the required values. **Note:** • Multiple values must be separated by a comma. • After enrollment, the cumulative count of SANs is displayed in the certificate property pop-up window from the holistic view.
***Organization**	The organization name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Organization Unit	Organization Unit name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
Locality	The locality name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.
State	The state name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on the configuration in the selected group's policy.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Country	Country name is one of the CSR parameters to be present in the certificate. This field will be auto-filled and editable based on configuration. It must be a 2-letter country code (for example, US, and so on). **Note:** For renewal of the certificate being enrolled, country name is required.
Email Address	Enter a valid email address of the person responsible for maintaining the certificate.
***Validity**	To specify the validity of the certificate being enrolled: a. From the first dropdown list, select the number of days/months/years. b. From the second dropdown list, select the unit of the duration from the following values: **Days**/**Months**/**Year**. For example, if the validity of the certificate is 2 months: i. From the first dropdown list, select **2**. ii. From the second dropdown list, select **Months**.
Challenge Password	Challenge password is one of the CSR parameters to be present in the certificate. Password must contain at least one alphabet (uppercase and lowercase), one number, and one special character.
Confirm Password	Re-enter the password entered in the **Challenge Password** field.
***Hash Function**	The Hash function with which the CSR has to be signed. Any information specific to any CA or vendor has to be covered in the Note section. This field will be auto-filled and editable based on the configuration in the selected group's policy. **Note:** For **Certificate Authority** = **HydrantID**, irrespective of the hash function selected, by default, the CA returns a certificate with SHA256. Therefore, admins must restrict users from creating a certificate with a hash function other than SHA256. To accomplish this, create policy with a single hash value (SHA256).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
***Key Type**	The key type is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
***Bit Length**	The bit length is used while creating a private and public key pair. This field will be auto-filled and editable based on the configuration in the selected group's policy.
**: Mandatory fields*	

6. In the **Attachments** section, upload any additional documents that are relevant to the enrollment of the certificate (for example, approval emails).

Field descriptions for the Attachments section

Field	Description
Name	Enter a name for the document. This need not be the actual name of the document; it can be an alternate name that will be used for reference only.
Comments	Enter any details relevant to the document being attached. **Note:** Character limit: **2000 characters**
Upload File	To upload an attachment: a. Click **Upload**. b. Navigate to the location of the document to be uploaded. c. Select the document to be document and click **Open**. The selected document is uploaded and listed in the table displayed below these fields in the **Attachments** section. **Tip:** If you've uploaded multiple attachments, use the **Search** field to find the required one.
**: Mandatory fields*	

7. In the **Certificate Attributes** section, enter organization-specific values, for the certificate attributes and custom attributes for the issuing CA, that need to be mentioned along with the CSR.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

These values will not be a part of the certificate but will be available in the AppViewX inventory. For example, cost center.

Note: This additional information can be used to filter certificate details in the inventory.

8. Enter the relevant details in the **Generic Fields**. These are default fields for maintaining the IP address and device information, if required.

Field descriptions for the Generic Fields

Field	Description
Device Name	Enter the name of the device.
Application IP Address	Enter the IP address of the application.
Tracking ID	A free-form business alpha-numerical identifier, included in the audit logs, that may be used to correlate audit log entries (typically enrollment and revocation events)
Certificate holder Email	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. An email address that may be used to send notifications to certificate holder depending on the notification policies configured for the requested workflow
First name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. First name (as a metadata) associated with the certificate to be enrolled
Last name	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Last name (as a metadata) associated with the certificate to be enrolled

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
Organization	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Organization name (as a metadata) associated with the certificate to be enrolled
Comment	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Additional information (as a metadata) associated with the certificate to be enrolled
UUID	**Note:** This field is displayed only when a CA setting with a registration authority is selected for certificate enrollment. Universal Unique Identifier, or UUID, (as a metadata) associated with the certificate to be enrolled

9. In the **Vendor-Specific Details** section, enter the CA-specific details. Some of the CAs will expect additional details other than CSR parameters as meta data for their operational purposes. Details common to all CAs will be taken from the AppViewX user information of the logged in user.

Field descriptions for the common vendor specific details

Field	Description
Certificate ID	The **Certificate ID** is auto-populated based on the value entered in the **Common Name** field (in the **CSR Parameters** section). • The **Certificate ID** can be modified by the user. • If the user edits the **Certificate ID**, any change to the **Common Name** will not reflect in the **Certificate ID**. • If the user deletes the **Certificate ID**, the value of the **Certificate ID** field is set to the **Common Name** suffixed with the timestamp.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the CSC Global CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Business Unit**	Enter the name of the business unit that is requesting the certificate.
***Organization Contact**	Enter the email address of the contact in the organization requesting the certificate.
***Phone Number**	Enter the phone number of the **Organization Contact** in the followung format: **+<country code>-<phone number>**. **Note:** For CSC Global, the phone number is not fetched from the AppViewX user information because of the difference in format.
***Domain Control Validation Type**	From the following options in the dropdown list, select the method CSC Global will use for authentication before issuing a certificate: • **EMAIL**: CSC Global will send an approval/confirmation request to the registered email ID. Certificate issuance happens only after approval is received. • **CNAME**: On requesting certificate issuance, CSC Global will provide you with a dynamic string. Add a CNAME record with this string to your DNS settings. CSC will issue the certificate requested only after validating this CNAME record. **Note:** CSC Global will perform domain validation for all CLM actions.
**: Mandatory fields*	

Field descriptions for the Custom CA vendor specific details

Field	Description
***CRL and OCSP required**	To control the inclusion of CRL and OCSP settings, turn this toggle button on/off as required.
**: Mandatory fields*	

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the DigiCert CA vendor specific details

Field	Description
***Server Type**	From the dropdown list, select the server on which the application that requires the requested certificate is hosted.
***Payment Method**	From the dropdown list, select one from the following payment methods: • **Bill To Account Balance**: This option allows you to pay for the DigiCert certificate using the available balance in your DigiCert account. **Note:** Ensure that the option to bill to account balance is enabled for the account and the account has sufficient balance. • **Bill To Default Credit Card**: This option will charge the cost of the DigiCert certificate to the credit card set as the default payment method in your DigiCert account. **Note:** Ensure that a credit card is configured as the default payment method for your account.
Additional Email	Enter email addresses that will receive notifications for renewals, reissues, and duplicates for the specified order.
Renewal Message	Enter a custom message that will be sent with the renewal notifications.
Notes	Enter a custom note that will be sent with the order.
**: Mandatory fields*	

Field descriptions for the DigiCert One CA vendor specific details

Field	Description
Seat ID	Enter the seat ID that will be assigned to the certificate being enrolled. Seat ID is a unique user-defined value assigned to identify an entity in the DigiCert One account. The seat ID for a certificate is used for certificate enrollment, renewal, and regeneration.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: The **Seat ID** field is displayed only if the **Allow Seat ID during enrollment** option is selected for the CA account. In this case, the value entered in the **Seat ID** field is now a unique identifier for the certificate being enrolled. Otherwise, a common seat ID is assigned to all certificates enrolled for the selected CA account

Field descriptions for the GlobalSign MSSL CA vendor specific details

Field	Description
***Profile name**	A profile name is defined at the time of creating an account on the GlobalSign MSSL portal. AppViewX retrieves all your profile names from the GlobalSign MSSL portal and populates them in this dropdown list. From the dropdown list, select the profile name the enrolled certificate should be mapped to.
**: Mandatory fields*	

Field descriptions for the Hydrant ID CA vendor specific details

Field	Description
Expiry Emails	Enter a comma-separated list of email addresses that will receive the certificate expiry notification from HydrantID. **Note:** HydrantID CA does not accept updates to these email addresses during the renewal process.

Field descriptions for the Nexus CA vendor specific details

Field	Description
Procedures	The **Procedures** dropdown list will display only the procedures mapped to the server and the default procedure. From the dropdown list, select the required procedure.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field descriptions for the LetsEncrypt CA vendor specific details

Field	Description
***Challenge Type**	Specifies the method for verifying domain ownership. Select the required domain for the validation. The available challenge types are: • **HTTP** • **DNS**.
Challenge Verify	Determines how the DNS challenge will be verified. Select the required verification process. The available challenge verifies are: • **Manual** • **Automatic**. The value **Automatic** suggests that the system will automatically handle the verification process without manual intervention. **Note:** This field appears when the challenge type is selected as **DNS**.
Vendor	Indicates the DNS provider responsible for managing DNS records. The available DNS service providers are: • **Cloudflare** • **Azure**. **Note:** This field appears when the challenge verify is selected as **Automatic**.
***Settings**	Allows for additional configuration settings related to the DNS challenge. The selected value **None** implies that no extra settings are applied. **Note:** This field appears when the challenge verify is selected as **Automatic**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Note: • Make sure that you have enabled **LetsEncrypt DNS Automation** from the workflow. • To add new vendors for the integration and configuration, refer to Integration topic in the Automation Guide.
**: Mandatory fields*	

10. Click **Add**.
    Once the details are added, you will be redirected to a page where the CSR and CA details are added as a connector. This page is called the holistic view and from here, any action on the certificate can be performed including provisioning the certificate to a server.
11. On the holistic view, click the **Submit** button to trigger the request.
    The submit action is triggered and the **Submit** dialog box is displayed.
12. Enter your comments in the text field and click **Yes**.
    If the approval required option is enabled in the CA policy, the request is moved to the **Approve** and **Implementation** stages.
13. Click **Approve** to proceed.
    The **Approve** dialog box is displayed.
14. Enter your comments in the text field.

    Note: If the workflow request has to be approved automatically in the future, click the **Schedule later** button .

15. Click **Yes**.
    Once the approval process is complete, the **Implement** option is displayed in the holistic view.
16. Click **Implement**.
    The **Implement** dialog box is displayed.
17. Enter your comments in the text field.
    If the workflow request has to be implemented automatically in the future, click **Schedule later** .
18. Click **Yes**.
    CSR Submission to CA is in progress.Once the CSR submission is successful, the request state will be changed to **Submit** certificate - retrieval in progress state.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

If the enrollment request is compliant with conditions defined and auto-approval enabled in the targeted CA, the certificate will be fetched in a few seconds.

If auto-approval disabled in the targeted CA, you will have to be logged into the CA and approve the request.

Once the certificate is issued successfully, the certificate will be retrieved into AppViewX. You can now push the enrolled certificate(s) to the required endpoint.

Adding and Pushing Certificates to Microsoft SQL Device

Important: Refer to the pre- and post-push script usage instructions here.

Adding an Application Connector for Microsoft SQL

MS SQL

1. On the certificate holistic view, click **Add Connector**.

2. Enter the **General Information** for the connector.

Field descriptions for the connector General Information

Field	Description
***Category**	From the dropdown list, select **Server**. If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the category selected at the time of certificate enrollment.
***Vendor**	From the dropdown list, select **MSSQL**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	If the certificate being pushed was enrolled with CSR generation at endpoint, this field is auto populated with the vendor selected at the time of certificate enrollment.
***Connector Name**	Enter a name for this connector, to be able to identify it later. **Tip:** AppViewX recommends naming connectors according to use cases so they are easily distinguishable.
Description	Enter any additional details you want to record for this connector.

Based on the information entered here, the **SSL templates** section is populated with the list of available MS SQL devices already onboarded in AppViewX.

3. To select the device(s) to which the certificate will be pushed, under **SSL templates**, from the list of **Available Devices**, click .
   The **Selected devices** list is updated automatically.
4. Enter the **Certificate Details**.

Field descriptions for the Certificate Details

Field	Description
Certificate Type	From the dropdown list, select the file type of the certificate to be pushed. AppViewX supports only PEM (*.crt) type as the certificate is imported to certificate store irrespective of the certificate type.
Push Root and Intermediate Certificates	To push the root and intermediate certificates, along with the end certificates, select this checkbox.
Private Key in Device	If the private key associated with the certificate being pushed has been stored on the **MS SQL machine**, select this checkbox.
***Key Location**	This field is displayed when the **Private Key in Device** option is selected. Enter the file path to the **private key** location on the **MS SQL machine**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Service Restart</td><td>Enabling this option will restart the SQL Server service to apply the configuration changes.

Note:
• By default, this setting is enabled based on the global device configuration. To modify, go to: CERT+ > Device Management > Server > Device Settings > Vendors > Microsoft SQL.
• This feature requires Windows Gateway version v2024.1.0.0 or later. In earlier versions, the service restarts automatically by default.</td></tr>
<tr><td>Force Encryption</td><td>Enabling this option enforces encryption for all SQL server connections.

Note:
• By default, this setting is enabled based on the global device configuration. To modify, go to: CERT+ > Device Management > Server > Device Settings > Vendors > Microsoft SQL.
• This feature requires Windows Gateway version v2024.1.0.0 or later. In earlier versions, the service restarts automatically by default.</td></tr>
<tr><td colspan="2">Note:
Bind Operation in AppViewX for MS SQL:
During the bind operation, AppViewX updates the registry with the following keys:
• Certificate Thumbprint Key: Stores the thumbprint of the pushed certificate.
• ForceEncryption Key: Set to 1 to enable encryption for the SQL instance.
After updating these keys, the SQL service is restarted to apply the changes.</td></tr>
</table>

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Note:

When pushing certificates , the system now automatically selects the appropriate PKCS12 encryption algorithm based on the target Windows Server version:

- **Windows Server 2016 and earlier**: Uses **TripleDES** encryption for compatibility
- **Windows Server 2019 and later**: Uses the encryption algorithm from General Settings

5. Enter the **Push Details**.

Field descriptions for the Push Details

Field	Description
***Script Location**	Script files are commonly used to perform certain tasks required to be completed before and/or after a certificate is pushed to the target system. The script to be run before the certificate is pushed is called a pre-push script and the script to be run after the push is called a post-push script. From the following options, select the location of the script file(s): • In AppViewX • In Device
Pre - Push Script File Name	Enter the file name of the pre-push script. **Important:** Read the pre and push script usage instructions here.
Pre - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the pre-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Post - Push Script File Name	Enter the file name of the post push script.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Field	Description
	Important: Read the pre and push script usage instructions here.
Post - Push Script File Path	This field is displayed when **Script Location** = **In Device**. Enter the location on your local system where the post-push script file is stored. **Important:** Read the pre and push script usage instructions here.
Push Automatically	To automatically push the certificate after it is renewed/reissued to the target system, enable this checkbox. **Note:** The auto push feature for a certificate works only if enabled for the certificate application connector as well the associated certificate group. To enable this feature at the certificate group level, refer the instructions here.

6. Click **Save**.
   The connector is displayed on the certificate holistic view.

What's Next

After adding the connector, you can proceed with pushing a server certificate to the device:

- To push a server certificate to a device, see Pushing a Server Certificate to a Device.

Pushing a Server Certificate to a Device

1. Go to (**Menu**) > **CERT+** > **CERTIFICATE ACTION** > **Push to Device** > **Server**.
   The **Server Certificate** page is displayed.
2. To push a certificate, under **Common Name**, click the required certificate.
   The certificate topology view is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

3. Click **Push to Device**. The Push to Device option will be shown if the app connector is already added to the certificate otherwise add the app connector and then proceed.

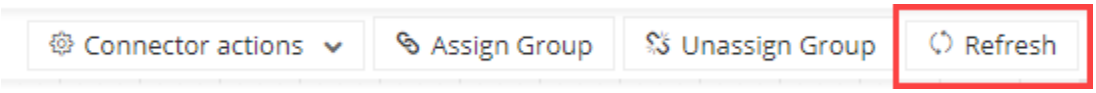
   Note: The **Push to Device** option is displayed only after an app connector is added to certificate.

   The **Confirmation** dialog box is displayed.
4. Enter your comments, if required, in the text field.
5. Click **OK**.
   - The approval process is triggered. The current flow is based on the default policy of two-level approvals.
   - A request ID and work order ID are generated automatically and the work order status is displayed alongside the connector in the certificate topology view.
6. To approve the push request, from the certificate topology view, click **Approve**.
7. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The work order status displayed beside the connector updates to **Push-Review In Progress**.
8. To implement the push request, from the certificate topology view, click **Implement**.
9. In the **Confirmation** dialog box:
   a. In the **Manual Implementation** field, to choose the mode of implementation, use the **On**/**Off** toggle.
   b. If you select **Off**, set the date and time to schedule the certificate push.
   c. Enter your comments in the text field and click **Yes**.

   The push action is triggered. After the push action is completed, the status updates to **Completed**.

   To refresh the certificate topology view, from the top-right corner of the screen, click **Refresh**.



Certificate Post script execution approach to Bind Certificates

Use the post-script execution method to bind certificates to SQL Server instances when using non-administrator or NT Service accounts for service logon.

If the SQL Server instance is running under a service account that is not 'Local System' or a member of the 'Administrators' group:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- Post Push Script:

```
$InstanceName = "MSSQLSERVER"  # Replace with your SQL instance name
$ServiceAccountName = "Domain\Username"  # Replace with actual account
$ForceEncryption = $true  # Set to $false if encryption should not be forced
$ServiceRestart = $true   # Set to $false to skip service restart

Write-Host "Checkpoint 1: Starting script"

# Decode and parse JSON
$request = [Text.Encoding]::Utf8.GetString([Convert]::FromBase64String($args[0]))
Write-Host "Checkpoint 2: Base64 decoded"

$request = $request.Replace('dNSNames','dNSNamesIgnore').Replace('iPAddresses', 'iPAddressesIgnore')
$json_request = ConvertFrom-Json -InputObject $request
Write-Host "Checkpoint 3: JSON parsed"

# Extract thumbprint
if (-not $json_request.certificate.extension.thumbPrint) {
    throw "Thumbprint field not found in JSON input."
}
$vmThumbPrint = $json_request.certificate.extension.thumbPrint.Replace(":", "")
$certificateThumbprint = $vmThumbPrint.ToLower().Replace(" ", "")
Write-Host "Checkpoint 4: Extracted thumbprint $certificateThumbprint"

try {
    # Load certificate
    $store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My", "LocalMachine")
    $store.Open([System.Security.Cryptography.X509Certificates.OpenFlags]::ReadOnly)
    $cert = $store.Certificates | Where-Object { $_.Thumbprint.ToLower() -eq $certificateThumbprint }

    if (-not $cert) {
        throw "Certificate with thumbprint $certificateThumbprint not found in LocalMachine\My store."
    }
    Write-Host "Checkpoint 5: Certificate loaded"

    # Verify private key
    if (-not $cert.HasPrivateKey) {
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    throw "The certificate does not have an associated private key."
}

# Locate private key file
$keyPath = $cert.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
$keyFullPath = "$env:ProgramData\Microsoft\Crypto\RSA\MachineKeys\$keyPath"

if (-not (Test-Path $keyFullPath)) {
    throw "Private key file not found at $keyFullPath."
}
Write-Host "Checkpoint 6: Private key path resolved $keyFullPath"

# Grant access to specified account
Write-Host "Checkpoint 7: Using provided service account: $ServiceAccountName"
$ntAccount = New-Object System.Security.Principal.NTAccount($ServiceAccountName)
$sid = $ntAccount.Translate([System.Security.Principal.SecurityIdentifier])
Write-Host "Checkpoint 8: SID resolved: $sid"

$acl = Get-Acl $keyFullPath
$accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule($sid, "Read", "Allow")
$acl.AddAccessRule($accessRule)
Set-Acl $keyFullPath $acl
Write-Host "Checkpoint 9: Granted Read access on private key to $ServiceAccountName"

# Set registry values
$sqlRegKey = Get-Item -Path 'HKLM:\Software\Microsoft\Microsoft SQL Server\Instance Names\SQL'
$sqlVersion = $sqlRegKey.GetValue($InstanceName)
if (-not $sqlVersion) {
    throw "SQL Server version key not found for instance $InstanceName."
}
Write-Host "Checkpoint 10: SQL version key resolved as $sqlVersion"

$sqlConfigPath = "HKLM:\Software\Microsoft\Microsoft SQL Server\$sqlVersion\MSSQLServer\SuperSocketNetLib"

Set-ItemProperty -Path $sqlConfigPath -Name "Certificate" -Type String -Value $certificateThumbprint

$forceVal = if ($ForceEncryption) { 1 } else { 0 }
```

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

```
    Set-ItemProperty -Path $sqlConfigPath -Name "ForceEncryption" -Type DWord -Value $forceVal
    Write-Host "Checkpoint 11: Registry updated - Certificate=$certificateThumbprint, ForceEncryption=$forceVal"

    # Optionally restart SQL service
    if ($ServiceRestart) {
        $sqlServiceName = if ($InstanceName -eq "MSSQLSERVER") { "MSSQLSERVER" } else { "MSSQL`$$InstanceName" }
        Restart-Service -Force $sqlServiceName
        Start-Sleep -Seconds 5

        $status = (Get-Service -Name $sqlServiceName).Status
        if ($status -eq "Running") {
            Write-Host "Checkpoint 12: Service $sqlServiceName restarted successfully."
            echo "AppResponseCode:0"
        } else {
            throw "Service $sqlServiceName failed to restart. Status: $status"
        }
    } else {
        Write-Host "Checkpoint 12: Service restart skipped as per input."
        echo "AppResponseCode:0"
    }
}
catch {
    Write-Error "An error occurred: $_"
    echo "AppResponseCode:1"
}
```

- The post-push script performs the following actions:
  - Grants read permission on the certificate's private key to the specified SQL Server service account.
  - Binds the certificate to the SQL Server instance using its certificate thumbprint.
  - Optionally:
    - Enables or disables **ForceEncryption** on the SQL Server instance.
    - Restarts the SQL Server service, if configured.
- **To bind a certificate to a SQL Server instance using a post-script**:
  - Place the script on the SQL Server where the certificate will be installed.
  - Update the following variables at the top of the script:
    - $InstanceName - Name of the SQL Server instance (for example, SQLEXPRESS or MSSQLSERVER).
    - $ServiceAccountName - The account under which the SQL Server service is running (for example, NT SERVICE\MSSQL$SQLEXPRESS or a domain account like domain\sqlsvc).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- $ForceEncryption - Set to $true to enable SSL encryption, or $false to disable it.
- $ServiceRestart - Set to $true to restart the SQL Server service after binding, or $false to skip the restart.

- In the AppViewX UI, while configuring the connector for MS SQL:
  - Select the Server Name (not the SQL instance name).
  - In the Push Details section:
    - Choose In Device.
    - Enter the full file path of the script placed on the server under Post-Push Script Filepath.

Note:

- You must manually update the $InstanceName, $ServiceAccountName, $ForceEncryption, and $ServiceRestart variables at the top of the script before executing it.
- The script is designed to be flexible and can be used with any SQL Server instance by modifying these variables as required.
- Optionally, you can create multiple versions of the script, each preconfigured for a specific SQL instance and service account, to simplify reuse across environments.

Enabling Auto Renewal of Certificates

To enable auto renewal of certificates, you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for pushing that certificate.

Note: While you can enable auto push for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto push for a server certificate.

1. To enable auto renewal for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
   The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
   The **Group : Modify : <group name>** page is displayed.

   c. From the **Other Details** section of this certificate group, turn on the **Renew Automatically** toggle button.

   d. Click **Update**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. To enable auto renewal for the certificate connector:

   a. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.

   b. From the inventory, for the certificate you want to enable auto renew for, click the common name.
   The holistic view of the selected certificate is displayed.

   c. For an existing CA connector for the certificate, hover over .

   d. From the menu displayed, click **Edit**.
   The certificate details are displayed.

   e. Under **CA Details**, turn on the **Renew Automatically** toggle.

   f. In the **Start Renewing** field, enter the number of days before expiration when the certificate should be renewed.

   g. Click **Update**.
   The holistic view of the selected certificate is displayed.

   > **Note:** For the auto renewal process to take effect, set the auto push in the application connector. For instructions, refer to the Enabling Auto Push section.

Enabling Auto Regeneration of Certificates

Enabling Auto Regeneration for a Certificate Group

You can enable and configure the auto regeneration feature at the certificate group level, which will apply to all certificates assigned to that group.

For details and instructions to enable auto regeneration at the certificate group level, click here.

Enabling Auto Regeneration at the Certificate Level

Enabling Auto Regenerate for Certificate Enrollment

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

For details and instructions to enable auto regeneration at the time of server certificate enrollment, click here.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Enabling Auto Regenerate for Discovered Certificates

While you can enable auto regenerate for all types of certificates, for clarity, in this section, we'll look at the instructions for enabling auto regenerate for a server certificate.

1. Go to **Menu** > **CERT+** > **Certificate Inventory** > **Server**.
   The **Server Certificate** inventory is displayed.
2. From the inventory, for the certificate you want to enable auto push for, click the common name.
   The holistic view of the selected certificate is displayed.
3. For an existing CA connector for the certificate, hover over ⋯.
4. From the menu displayed, click **Edit**.
   The certificate details are displayed.
5. Under **CA Details**, turn on the **Regenerate Automatically** toggle.
6. In the **Start Regenerating** field, enter the number of days before expiration when the certificate should be regenerated.
7. Click **Update**.
   The holistic view of the selected certificate is displayed.

> **Note:** For the auto regenerate process to take effect, set the auto push in the application connector. Refer to the Enabling Auto Push section.

Enabling Auto Push of Certificates to Endpoints

After setting the auto renew/regenerate in the CA connector, you must now enable the auto push in the application connector to ensure the renewed/regenerated certificates are pushed to the end device.

To enable auto push of certificates, **you need to enable the corresponding option for the group to which the certificate in question belongs, as well as the connector created for that certificate**.

1. To enable auto push for the certificate group:

   a. Go to **Menu** > **CERT+** > **Groups & Policies** > **Groups**.
      The **Group** page is displayed.

   b. From the **Name** field, select the required certificate group.
      The **Group : Modify : <group name>** page is displayed.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

c. From the **Other Details** section of this certificate group, turn on the **Push Certificate Automatically** toggle button.

d. Click **Update**.

2. To enable auto push for the certificate connector:

a. From the holistic view, for an existing application connector for the certificate, hover over **(More)** icon.
To add an application connector, follow the instructions given here.

b. From the menu displayed, click **Edit**.
The **Edit Application Connector** pop-up is displayed.

c. Select the **Push automatically** checkbox.

> **Important:** The auto-push feature works only when it is enabled at the connector level and disabled at the group level. If enabled at the group level but disabled at the connector level, the feature will not function.

d. Click **Save**.
The holistic view of the selected certificate is displayed.

> **Note:** An **Auto Renew Certificates** job is scheduled to run every 6 hours. It auto renews the configured certificates based on the number of days before expiry. AppViewX will disable the push automatically option in the Parent certificate application connector and enable it in the renewed certificate application connector.

> **Note:** An **Auto Regenerate Certificates** job is scheduled every day. It auto regenerates the configured certificates based on the number of days before expiry.

Troubleshooting MS SQL Windows

This section helps you troubleshoot the common problems that you might encounter when using certificate server functionalities. This guide will give more troubleshooting processes on server addition, deletion, import, export, push, bind, rollback and other actions associated with MS SQL Windows.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Issues in Communicating to MS SQL

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
Communication to <hostname> has failed	Hostname or Credentials configured is wrong	Ensure hostname and the device credentials configured while device addition is valid.
Device version fetch has failed.	MSSQLSERVER service instance is down	Restart the MSSQLSERVER instance
Device version fetch has failed.	Command not supported by MS SQL version	Execute the version command SQLCMD -Q 'SELECT @@VERSION;' -t 3 in the CLI of the device to check if it returns version response

Issues in Config Fetch

Error Message	Possible Cause	Possible Solution
Communication to <hostname> has failed	Gateway agent not reachable. Device not reachable from the gateway agent	Ensure gateway is configured properly and the APIs are accessible from AppViewX. Ensure device and gateway agent are in the same domain and device is accessible from gateway agent.
PTPLD178 has 0 instances.	No installed MS SQL instances.	Execute (get-itemproperty 'HKLM:\\SOFTWARE\\Microsoft\ \Microsoft SQL Server').InstalledInstances in the device as a powershell script and check if it returns the MS SQL instances

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Error Message	Possible Cause	Possible Solution
	Installed instances are not up and running.	

Issue in Discovery

Error Message	Possible Cause	Possible Solution
Received failed response from batch	No valid certificates in store that are binded to the MS SQL instances.	Ensure the certificates are binded to a MS SQL instance.

Issue in CSR generation

Error Message	Possible Cause	Possible Solution
CSR Submission Failed	User may have restricted access to the path configured for the “CSR FileName” and “Key File name”	Kindly ensure the user configured for device addition has read/write access to the path configured.

Issue in Push and Rollback

Error Message	Possible Cause	Possible Solution
Error while pushing certificate in Device : <device name>.PrivateKey not available.	Private key is not available to parse certs.	Kindly ensure to push certs with private key.If privatekey is available in device please select privateKeyInDevice option.
Error: “/LOCAL_MACHINE/ CertificateAuthority” does not exist	CertificateAuthority Store is removed from the Store	Create a CertificateAuthority store.

AppViewX Integration with MDM devices

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Certificate Lifecycle Management with Mobile Device Management (MDM)

Mobile Device Management

Mobile Device Management (MDM) is a type of security software used by IT departments to monitor, manage, and secure employees' mobile devices such as smartphones and tablets. It involves the following steps:

- **Enrollment** - This step includes enrolling the mobile device into the MDM system. This can be done manually by the user or automatically through methods such as QR codes, email links, or by connecting to a company network.
- **Configuration** - Administrators create configuration profiles that define the settings and policies for the devices. These profiles can include Wi-Fi settings, VPN configurations, email settings, and more.
- **Deployment** - Once profiles and policies are created, they are pushed to the enrolled devices. This can happen over the air (OTA) through cellular or Wi-Fi connections.
- **Management** - Administrators can remotely manage the devices. This includes pushing updates, locking or wiping devices if they are lost or stolen, and troubleshooting issues.
- **Security** - MDM ensures that corporate data is protected through encryption, secure access controls, and the ability to remotely wipe data if a device is compromised.
- **Compliance** - Administrators can generate reports and audit trails to ensure compliance and for review purposes.

Integration of Mobile Device Management (MDM) with Auto-Enrollment Protocols

Mobile Device Management (MDM) systems often support auto-enrollment protocols like SCEP, EST, etc to streamline the process of enrolling devices into the management system. Auto-enrollment simplifies the initial setup for users and ensures that devices comply with organizational policies from the moment they are activated.

Benefits of using MDM with Auto-Enrollment Protocols:

- **Automation** - Automates the certificate issuance and renewal process, reducing administrative overhead and minimizing the risk of errors.
- **Scalability** - Easily scales to manage certificates for a large number of devices.
- **Seamless User Experience** - Provides a seamless experience for users, who don’t need to manually request or install certificates.

Use Cases:

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

- **Wi-Fi Authentication** - Devices use certificates to authenticate to secure Wi-Fi networks, ensuring only authorized devices can connect.
- **VPN access** - Certificates authenticate devices when connecting to corporate VPNs, providing secure remote access.
- **Email encryption and signing** - Certificates enable secure email communications by supporting encryption and digital signing.
- **Application Authentication** - Certificates authenticate devices and users to enterprise applications, ensuring secure access to sensitive data.

Some of the most popular MDMs that AppViewX integrates with are:

- **Microsoft Intune** - Part of the Microsoft 365 Suite, Intune provides comprehensive MDM and mobile application management (MAM) capabilities. Supports Windows, iOS, Android, and macOS devices.
- **Jamf Pro** - A leading MDM solution for Apple devices, widely used in enterprise and education settings. Supports macOS, iOS and iPadOS.
- **MobileIron** - A UEM platform that focuses on securing endpoints, apps, and cloud services. Support for iOS, Android, Windows, and macOS.

AppVewX Integration with JAMF

What is JAMF

The advantages of using Jamf are as follows:

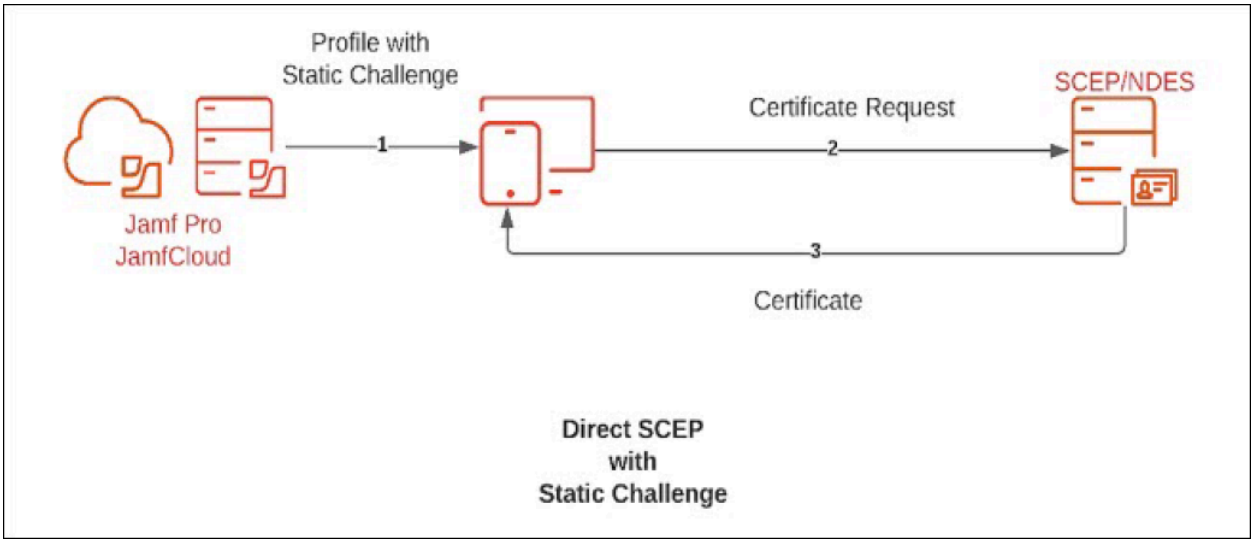
- **The Industry Standard for Apple Device Management** - The various products in the Jamf suite allow for seamless setup and deployment of devices, all offered in a single consolidated solution.
- **Cloud-Based Mobility** - Jamf Now is the ideal solution for small and medium enterprises as it empowers setting up, protecting, and managing devices right from one product.
- **Device Management Tool for The Pros** – An ultimate EMM (Enterprise Mobility Management) tool for your users. Jamf Pro features application and device management, deployment, security capabilities, inventory collection, and more.
- **Enhanced Identity Management** - Jamf Connect offers the flexibility to remotely and centrally manage passwords, groups, and users. It provides access to corporate cloud resources and applications that offer an advanced security and identity approach.
- **Mac-Exclusive Endpoint Protection** - Jamf Protect, developed natively on the iOS architecture offers deep visibility into any operations or threats at the endpoints. It has a dashboard, extensive reporting, and real-time alerts on the built-in security framework for macOS.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Deployment Models

SCEP obtains certificates from the CA and distributes them to managed mobile devices, providing a simplified way of handling large-scale certificate distribution. If you do not want computers or mobile devices to communicate directly with a SCEP server, you can configure settings that enable Jamf Pro to proxy the communication between a SCEP server and the computers and mobile devices in your environment. This allows Jamf Pro to communicate directly with a SCEP server to obtain certificates and install them on the device.

Jamf Pro can be configured using computers or mobile devices to communicate directly with a SCEP server.



Prerequisites

1. Disabling the checkbox in the **Global Management** > **PKI Certificates** screen.

    a. Login to JamfCloud (Sample URLs are mentioned below):
        i. **Cloud-hosted**— https://JAMF_PRO_URL.jamfcloud.com
        ii. **On-premise**— https://JAMF_PRO_URL.com:8443

    b. Click **Settings** > **All Settings** > **Global Management** > **PKI Certificates**.

    c. Ensure to disable the checkbox labeled **Enable Jamf Pro as SCEP Proxy for configuring profiles**.

    > **Note:** This is an important step to enable this deployment model.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

2. Configure the **Challenge Password** in the **SCEP Configuration** and **AppViewX** endpoints.

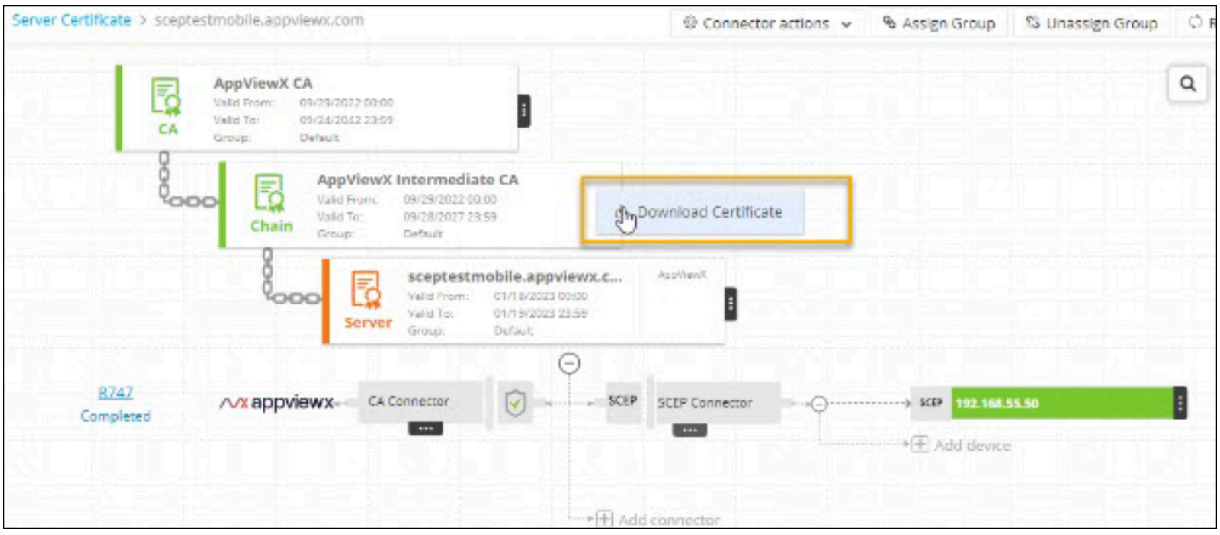
> **Note: Challenge Passphrase** is mandatory for MAC devices to connect to AppViewX SCEP Node.

3. The MAC device should be able to connect to the SCEP server on port 30022.

Direct Communication with SCEP Server

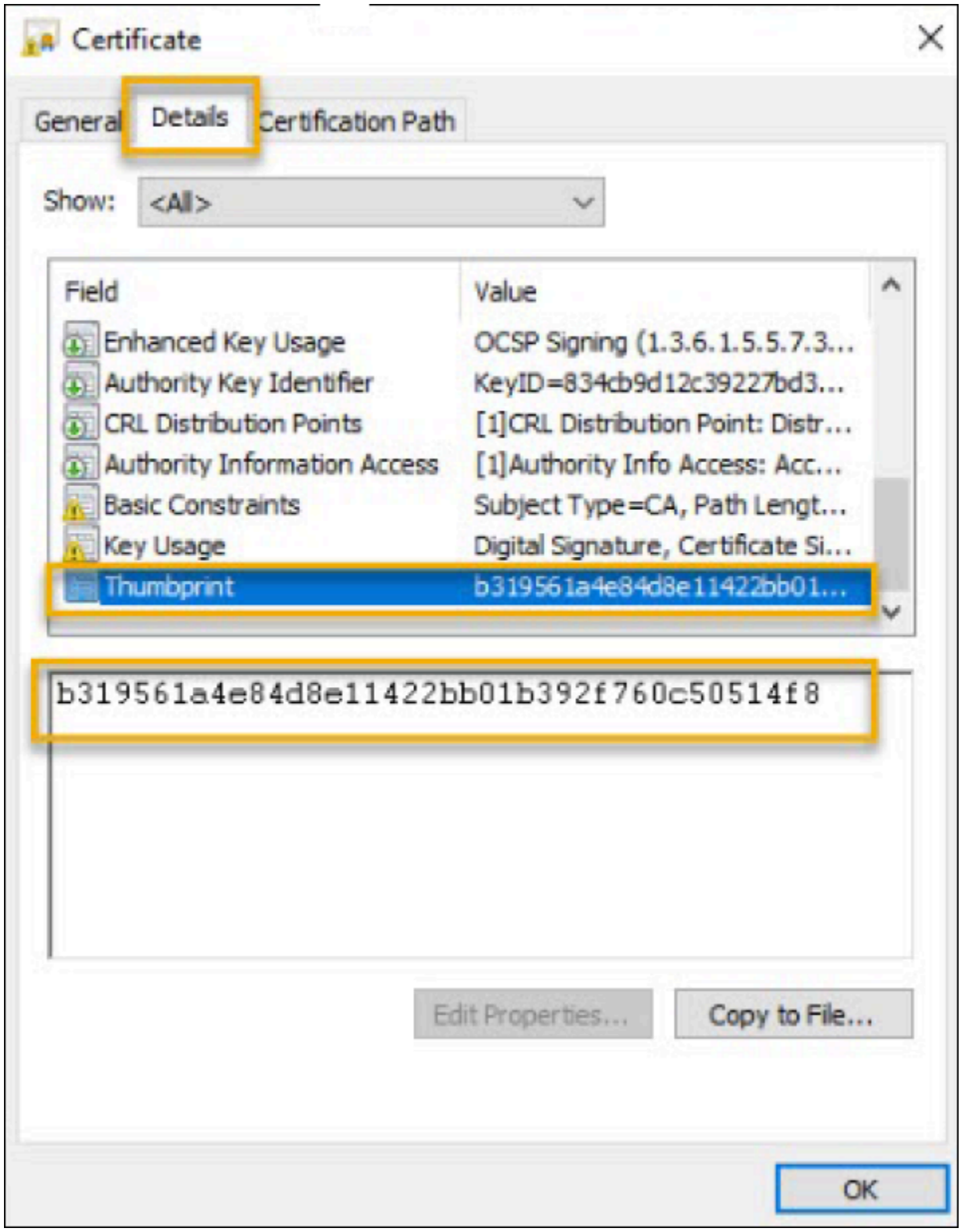
Obtaining the Certificate Thumbprint/Fingerprint

1. Log in to the AppViewX platform using valid credentials.
2. Hover on the menu icon and select CERT+.
3. Click **Certificate Inventory** on the left menu and select the certificate type (Server, Client, or Code Signing).
   The certificates with the common names are displayed on the right.
4. From the **Common Name** column, click on the desired certificate.
   All valid certificates are displayed.
5. Click the desired RA certificate to display the details.



6. Click the three dots on the issuer certificate to display the **Download Certificate** option.
7. Click **Download Certificate** and save the certificate in the desired format.
8. Open the downloaded certificate.

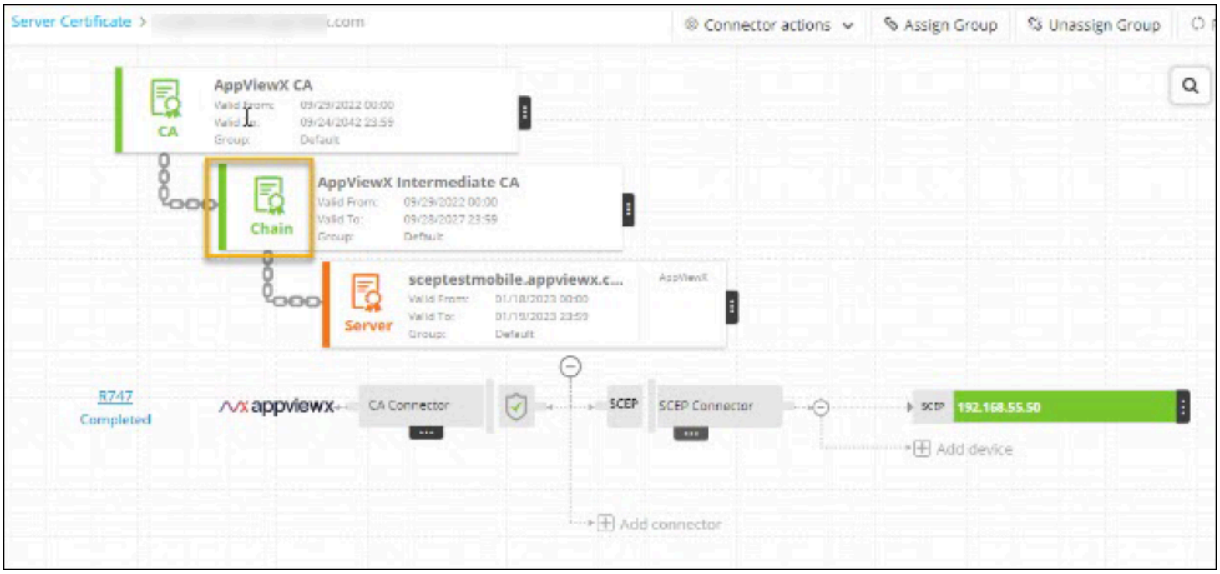
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



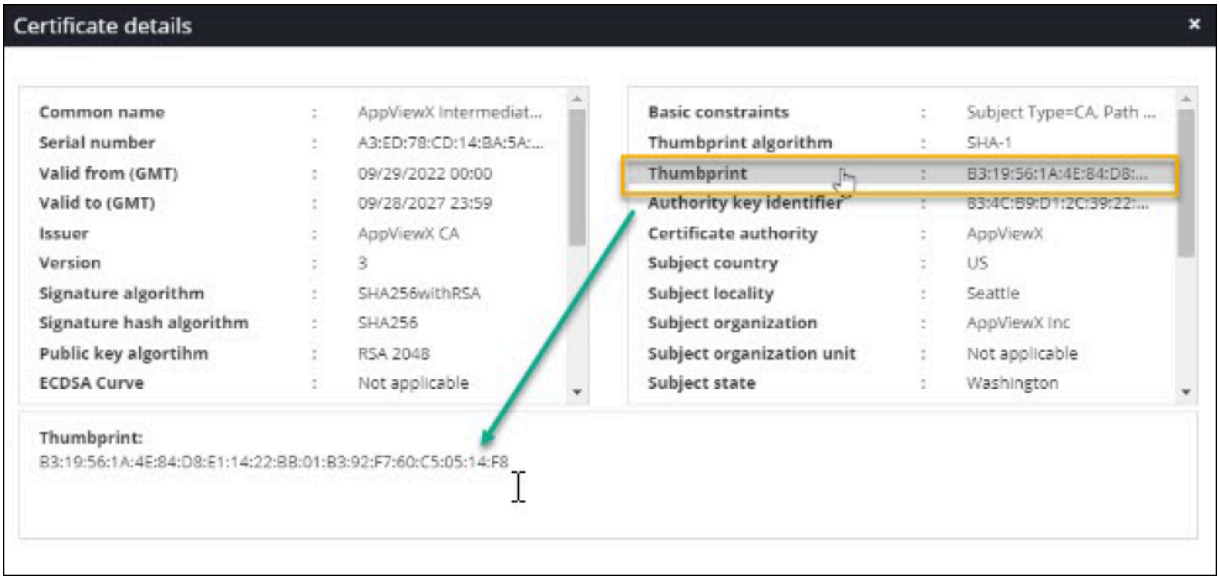
9. Click the **Details** tab and then select the Thumbprint field.
   The full value is displayed in the section below.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. Copy this hex value and paste in the text pad. Use this value in the Fingerprint field in JAMF Pro (described in the section below).
    Consequently, another way to obtain the hex value without having to manually delete the colons in the thumbprint can is described below.
11. Execute steps 1 to 5 described above.



12. Click the Issuer certificate.

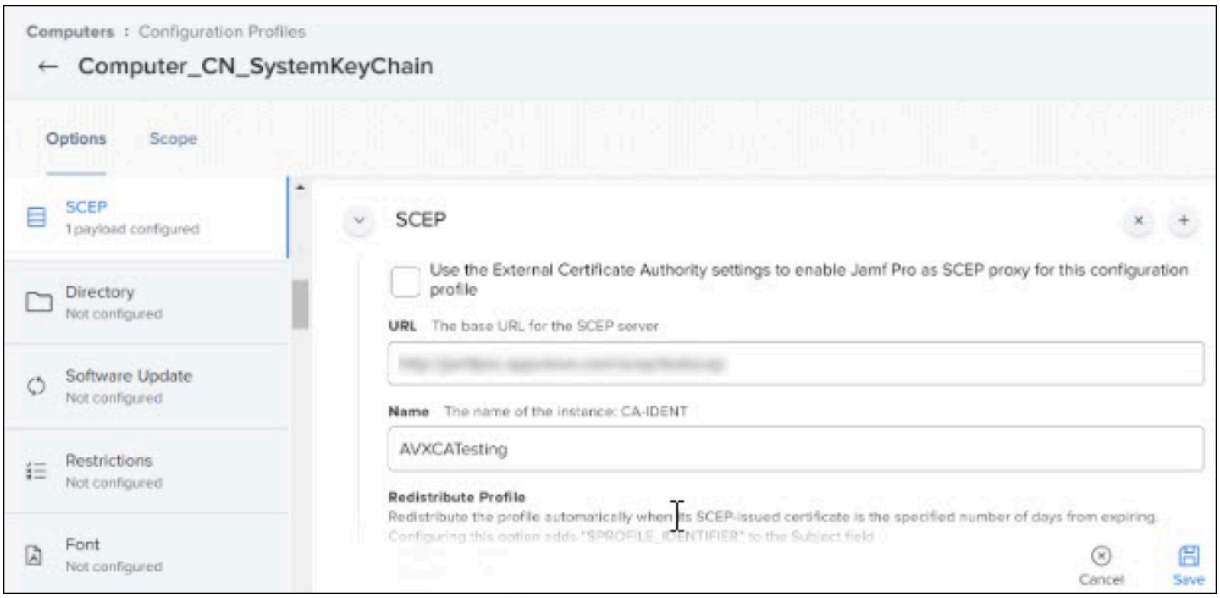


13. In the Certificate Details pop-up, click the **Thumbprint** value.
    The full value is displayed in the section below.
14. Copy this hex value and paste in the text pad. Ensure to remove all the colons before using it in the Fingerprint field in JAMF Pro (described in the section below).

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

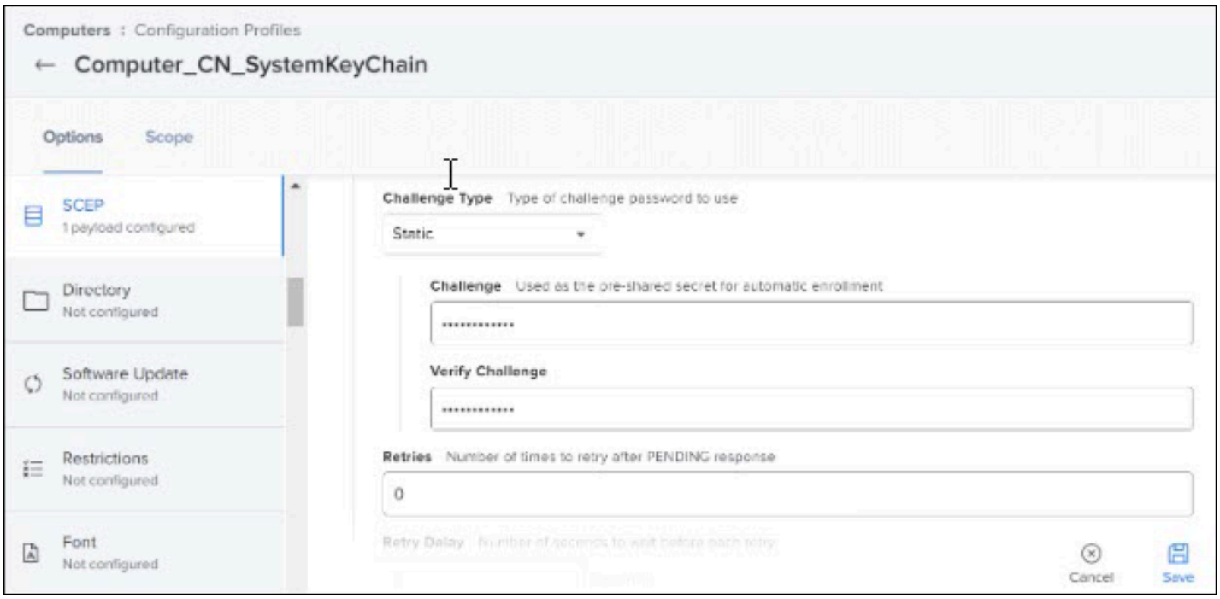
Configuring SCEP

1. Navigate to **SCEP Configuration Profiles** screen.



2. In the **URL** field, enter the AppViewX server's publicly exposed SCEP URL.
3. In the **Name** field, enter the desired name for this configuration.
4. From the **Redistribute Profile** dropdown, choose a value to specify the number of days before the certificate needs to be renewed. For example, if you want a certificate to be renewed 15 days before expiry, then set the **Redistribute Profile** to 15 days.
5. In the Subject field, enter the variable names. The $ (dollar) sign may be used with the variable name. Refer to the Mobile Device Configuration Profiles page to learn about the variable names supported in Jamf.
6. From the **Subject Alternative Name Type** dropdown, select *None*.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



7. From the Challenge Type dropdown, select the following:

   a. **Static** - If you want all computers and mobile devices to use the same challenge password, choose “Static” and specify a challenge password. The challenge password will be used as the pre-shared secret for automatic enrollment.

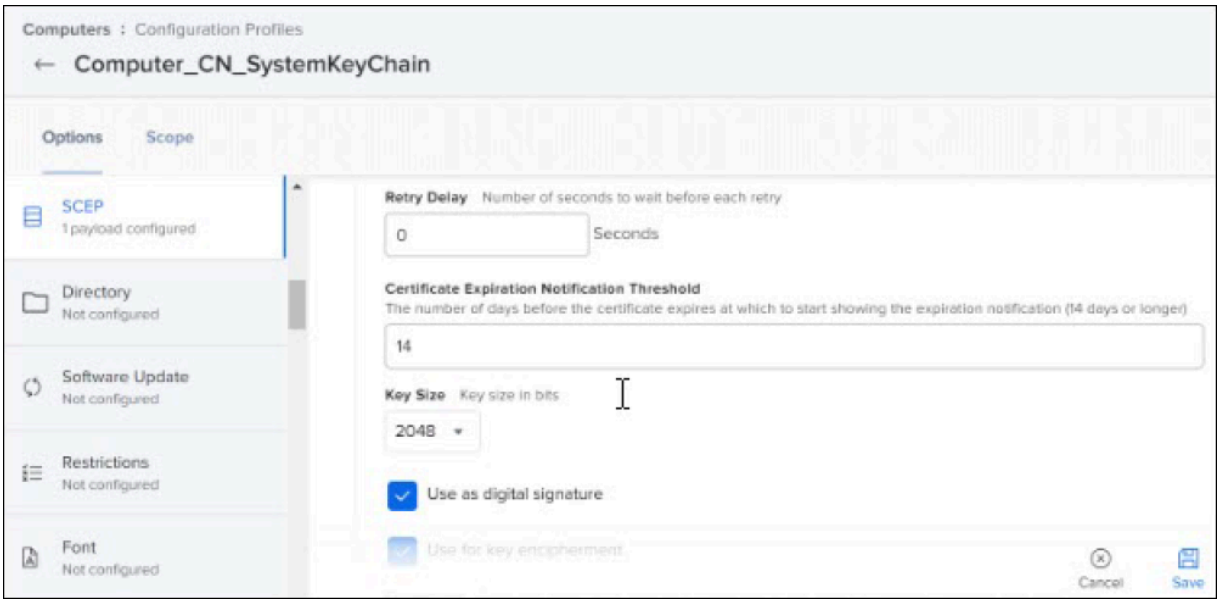
   b. **Dynamic** - If you are using a non-Microsoft CA and you want each computer and mobile device to use a unique challenge password, choose “Dynamic”. The Dynamic challenge type requires use of the Classic API and membership in the Jamf Developer Program. The Dynamic challenge uses the "Fingerprint" or "Thumbprint" to authenticate the user instead of a username and password. The Thumbprint hash value for the **Fingerprint** field in Jamf Pro can be found on the profile you receive. Before selecting this option, contact your Jamf account representative to learn more about the Jamf Developer Program and the additional steps you need to take to use this option.

   > **Note:** Currently, CERT+ does not support the dynamic challenge passphrase.

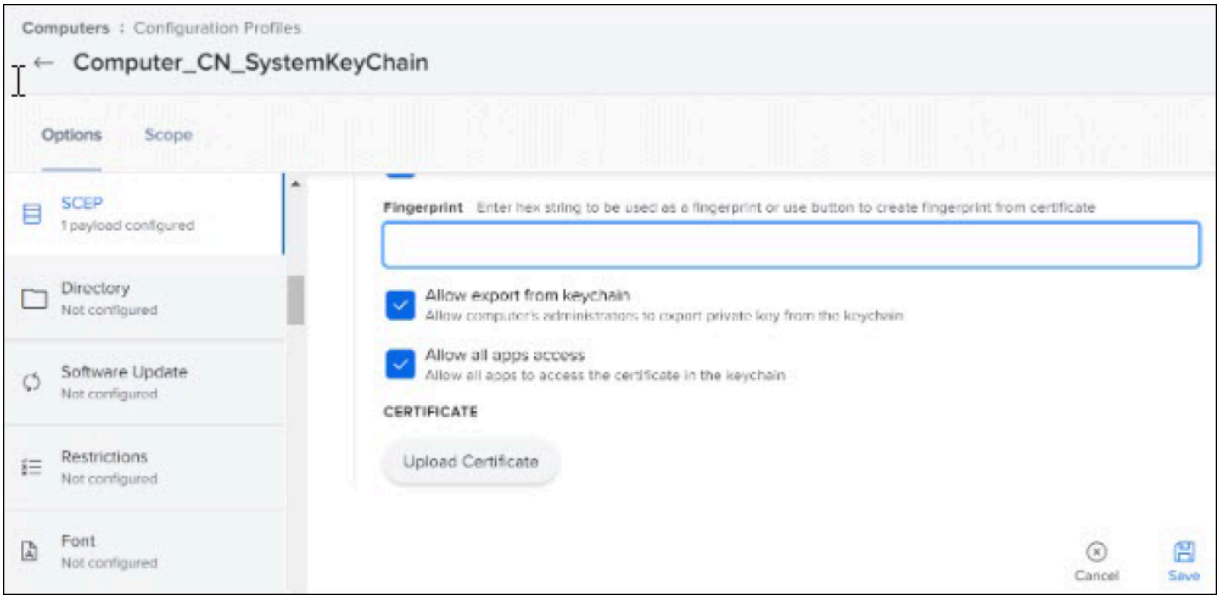
8. In the **Challenge** and **Verify Challenge** fields, enter the AppViewX SCEP Challenge Password configured in AppViewX SCEP UI.

> **Note:** This is a mandatory step. The Challenge password is mandatory while using this deployment model. The same challenge password set in the prerequisite should be configured in the JAMF.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

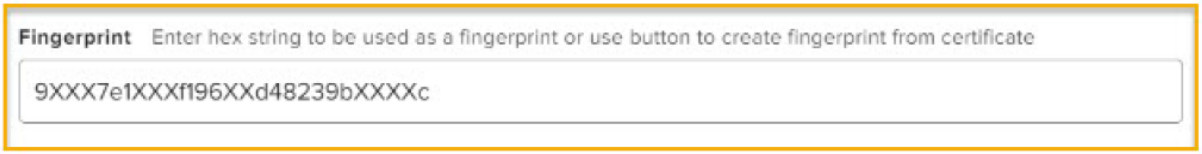


9. In the **Retry Delay** field, enter a desired value (in seconds).
10. In the **Certificate Expiration Notification Threshold** field, enter the number of days before the certificate expiration at which a notification will start displaying.
11. From the **Key Size** dropdown, select value *2048*.
12. Select the checkboxes **Use as digital signature** and **Use for key encipherment**.



13. In the **Fingerprint** field, enter the hex string to be used as a fingerprint.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

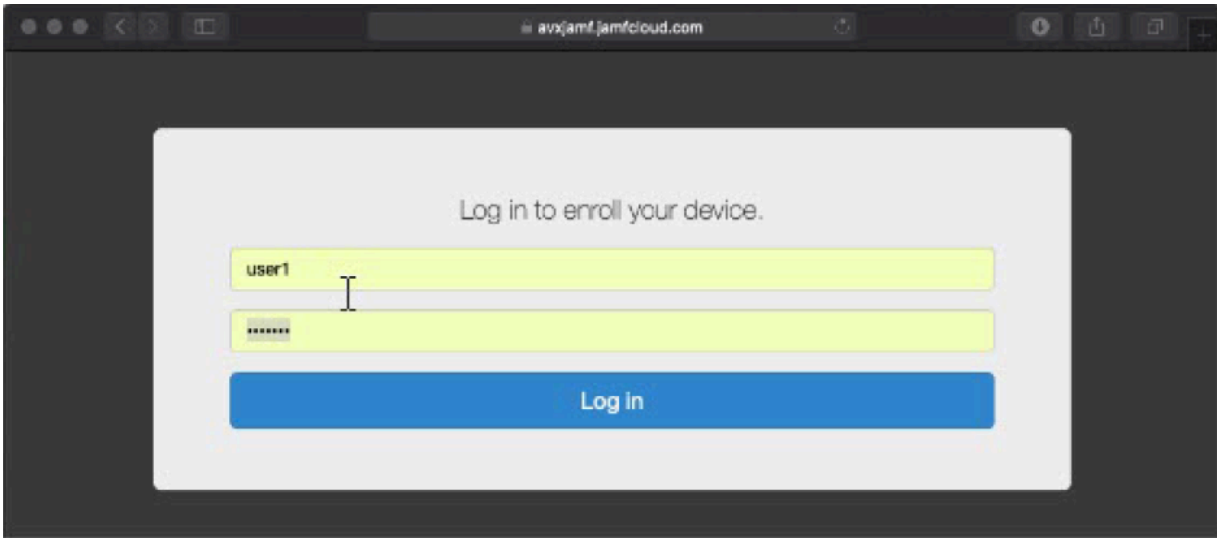


14. Select the checkboxes **Allow export from keychain** and **Allow all apps access**.
15. Click **Save**.

Initiating the Enrollment from a Device

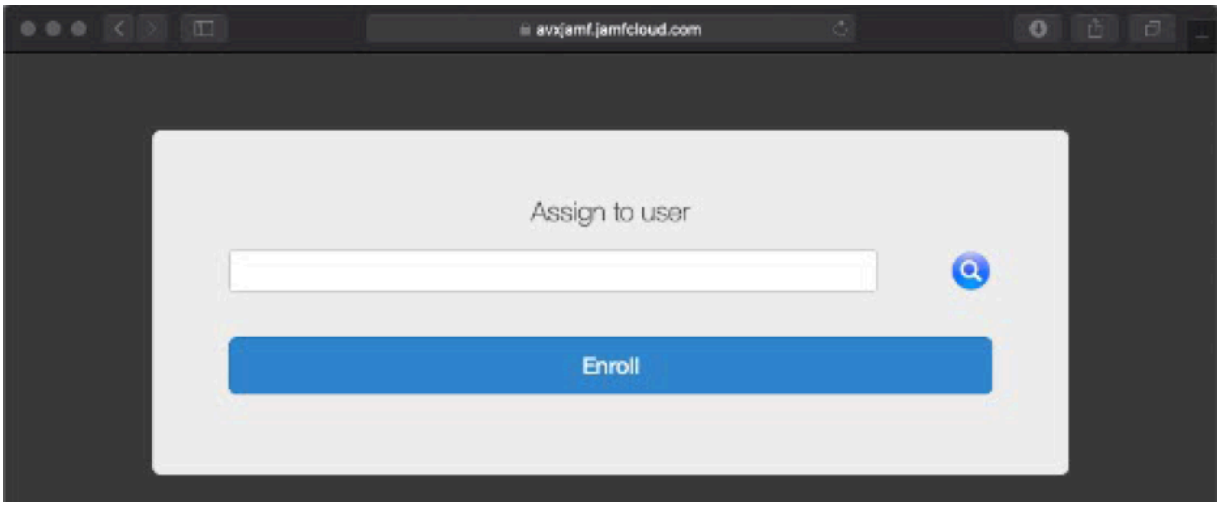
This section provides details of testing the Jamf cloud configuration performed in the previous section. It is recommended to open the JamfPro Enrollment URL using a Safari browser, as other browsers are not capable of identifying the received configuration profile and installation to the machine. Follow the instructions shown in the MacOS screen.

1. Enter the URL, for example - https://avxjamf.jamfcloud.com/enroll/ in the Safari browser.
2. Enter a valid username and password.

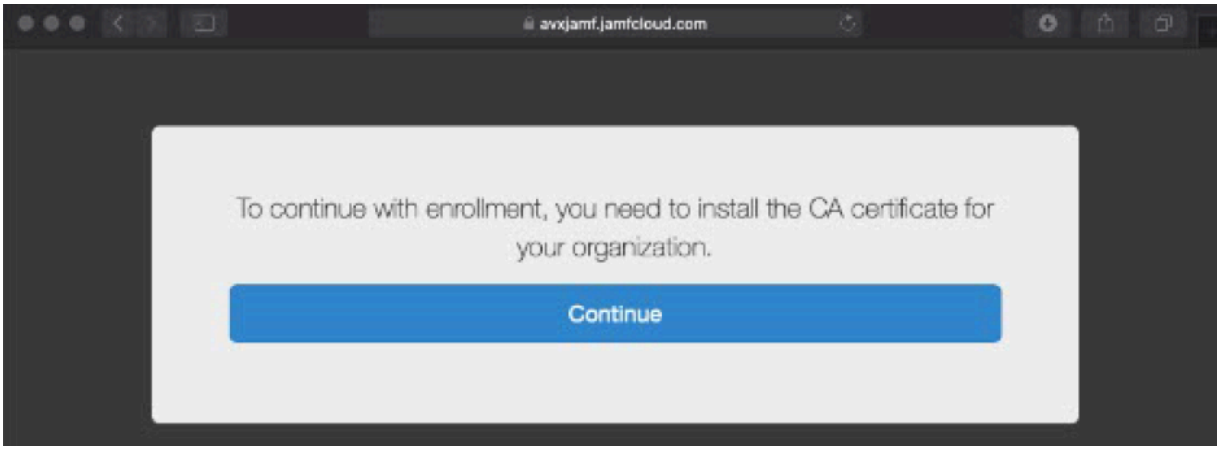


3. Leave the **Assign** to user field empty and click **Enroll**.

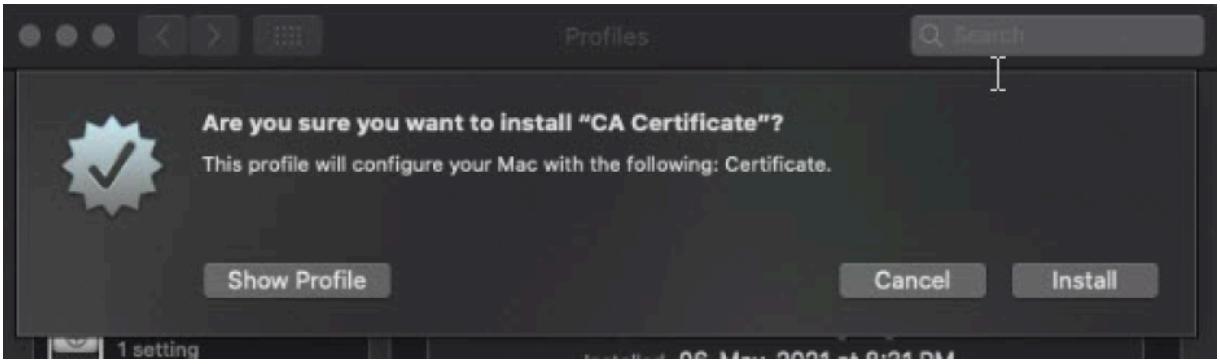
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



4. To continue with the enrollment (installation of CA certificate), click **Continue**.

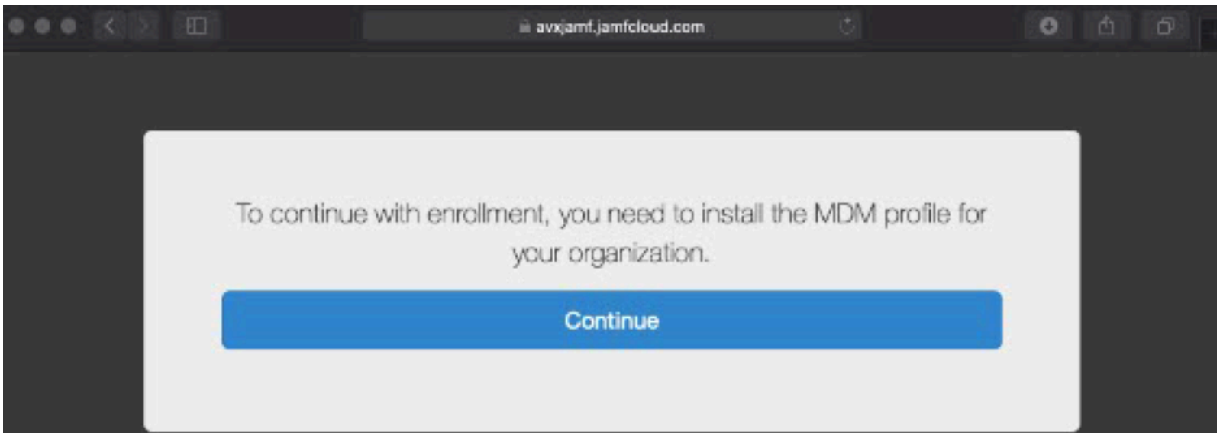


5. To confirm installation of the CA Certificate, click **Install**.

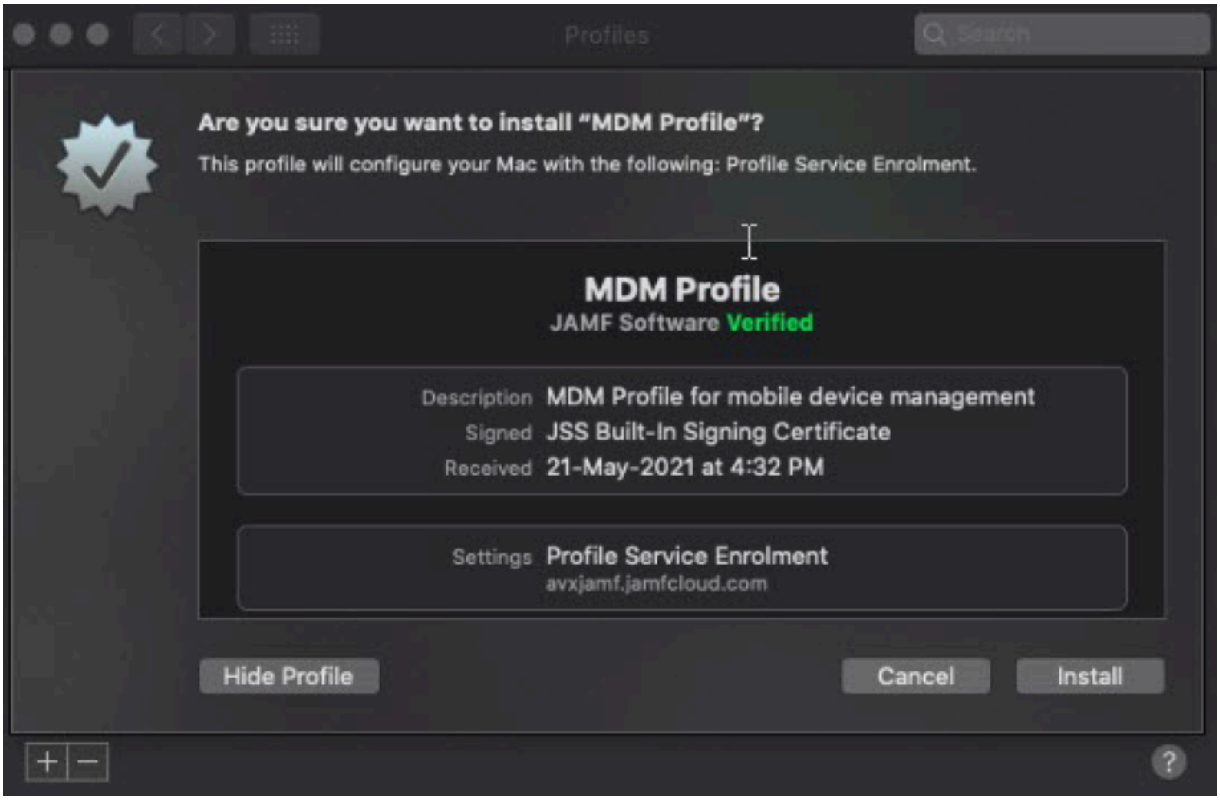


6. To continue with the enrollment (installation of the MDM profile), click **Continue**.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



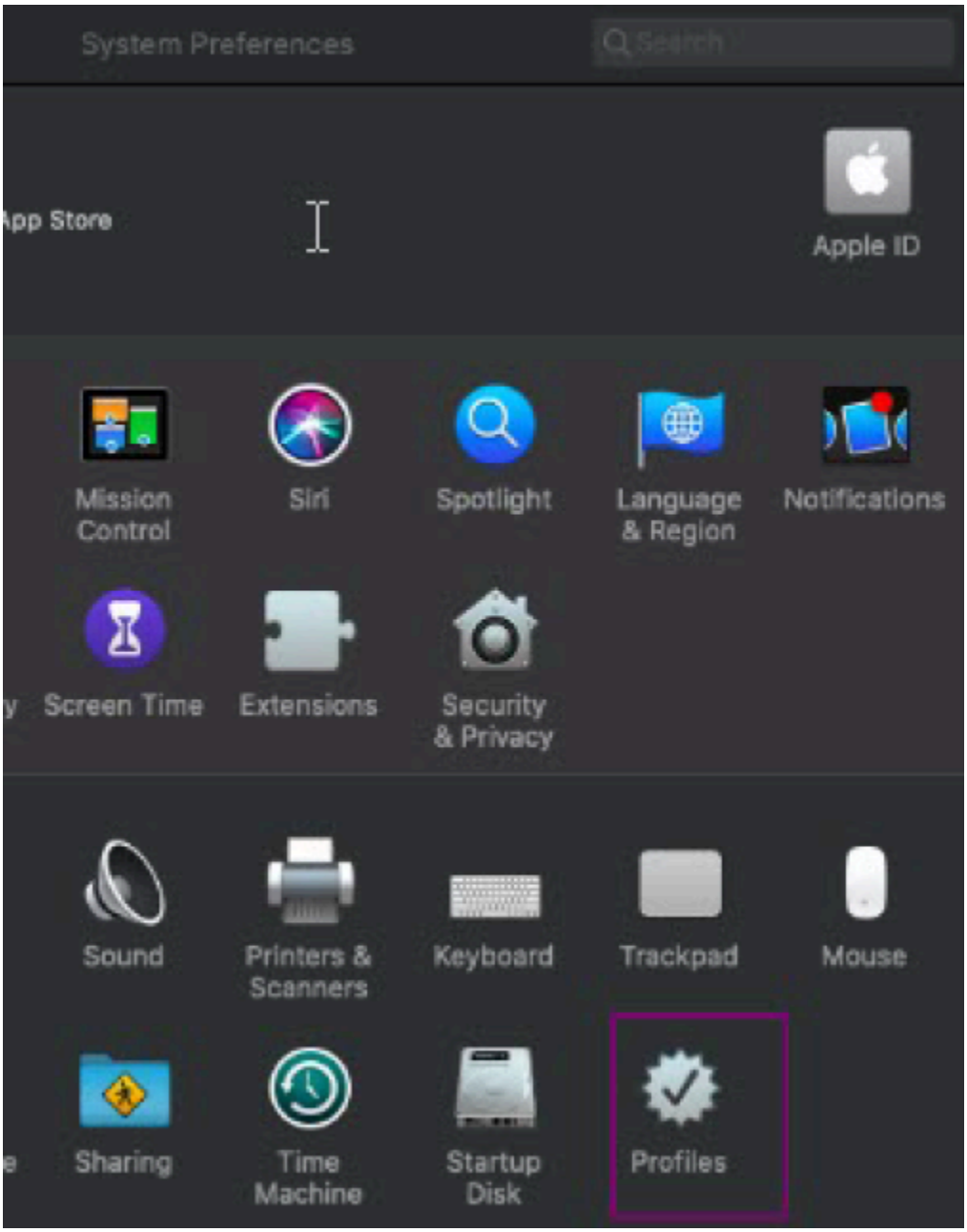
7. To confirm installation of the MDM Profile, click Install, and enter the valid credentials to carry out the installation.



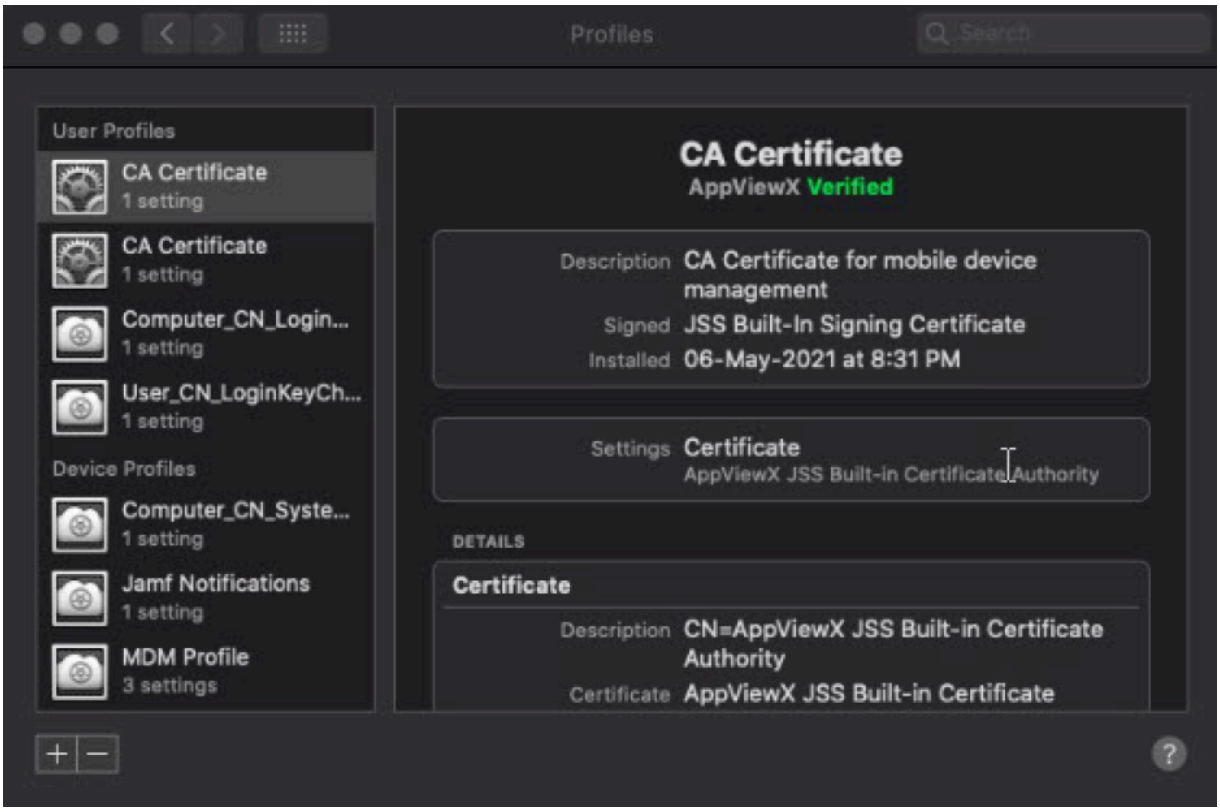
8. After the installation is complete, the following message is displayed – "The enrollment process is completed."
9. Wait for approximately one minute for the installation of the Profile and Certificate. (Profile contains SCEP configuration and during the installation process, the device directly sends a SCEP request to the AppVIewX Server.)

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

10. After the installation, the profiles can be verified by clicking **System Preferences** > **Profile**. All the installed profiles must be visible.



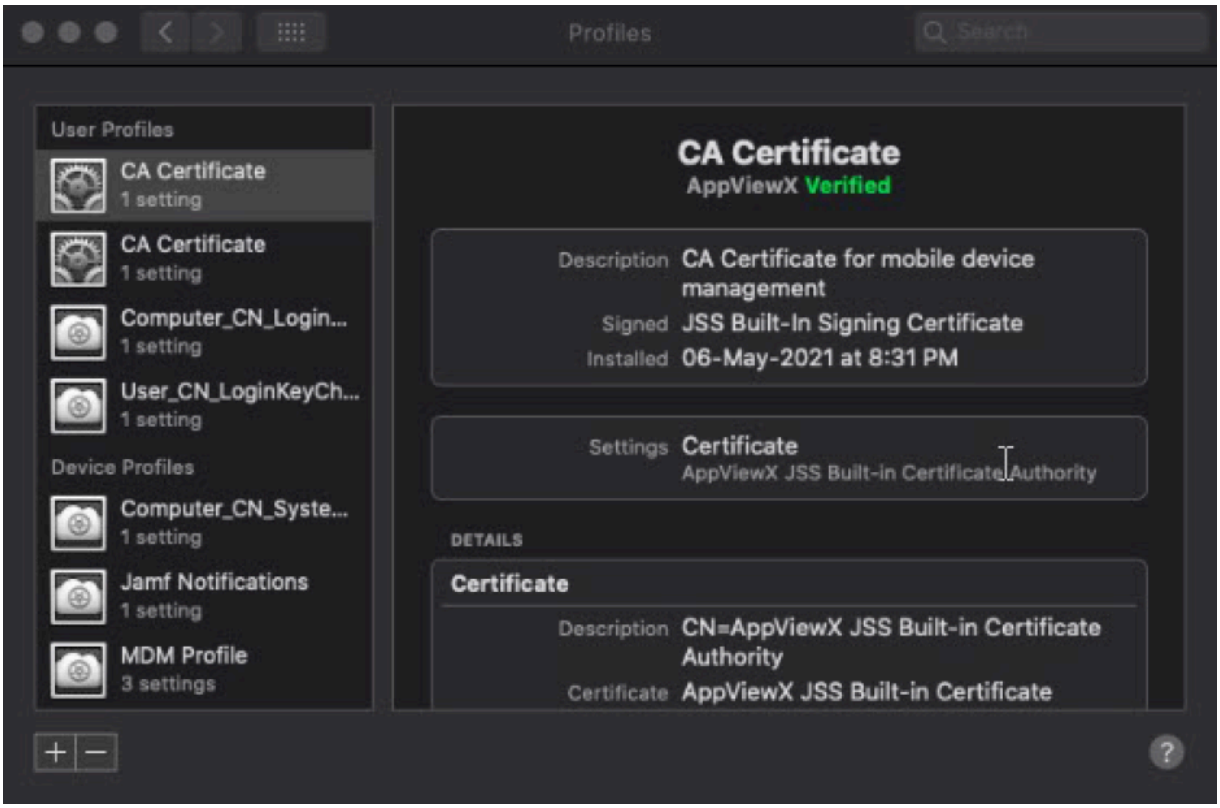
Copyright © 2025 AppViewX, Inc. All Rights Reserved.



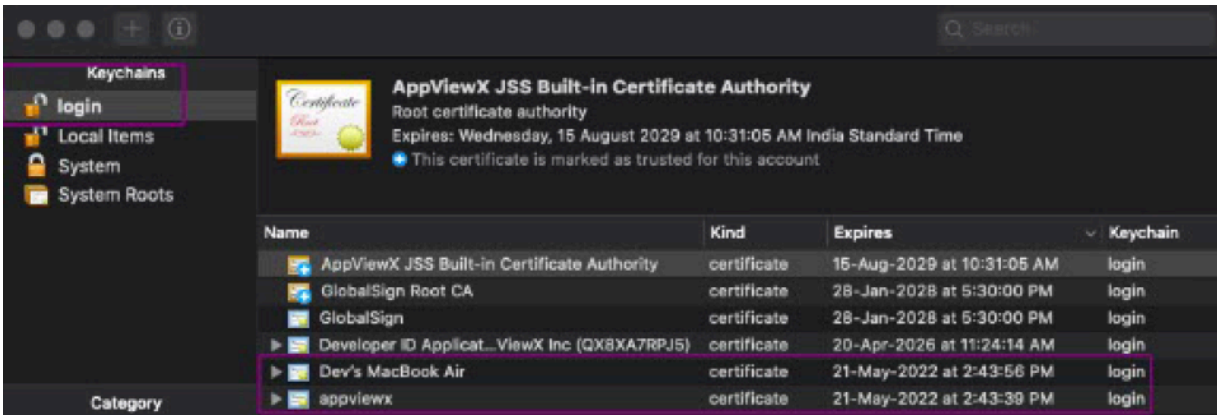
Note: Deleting the MDM profile deletes all the information from the Profiles. A fresh enroll may be tried later.

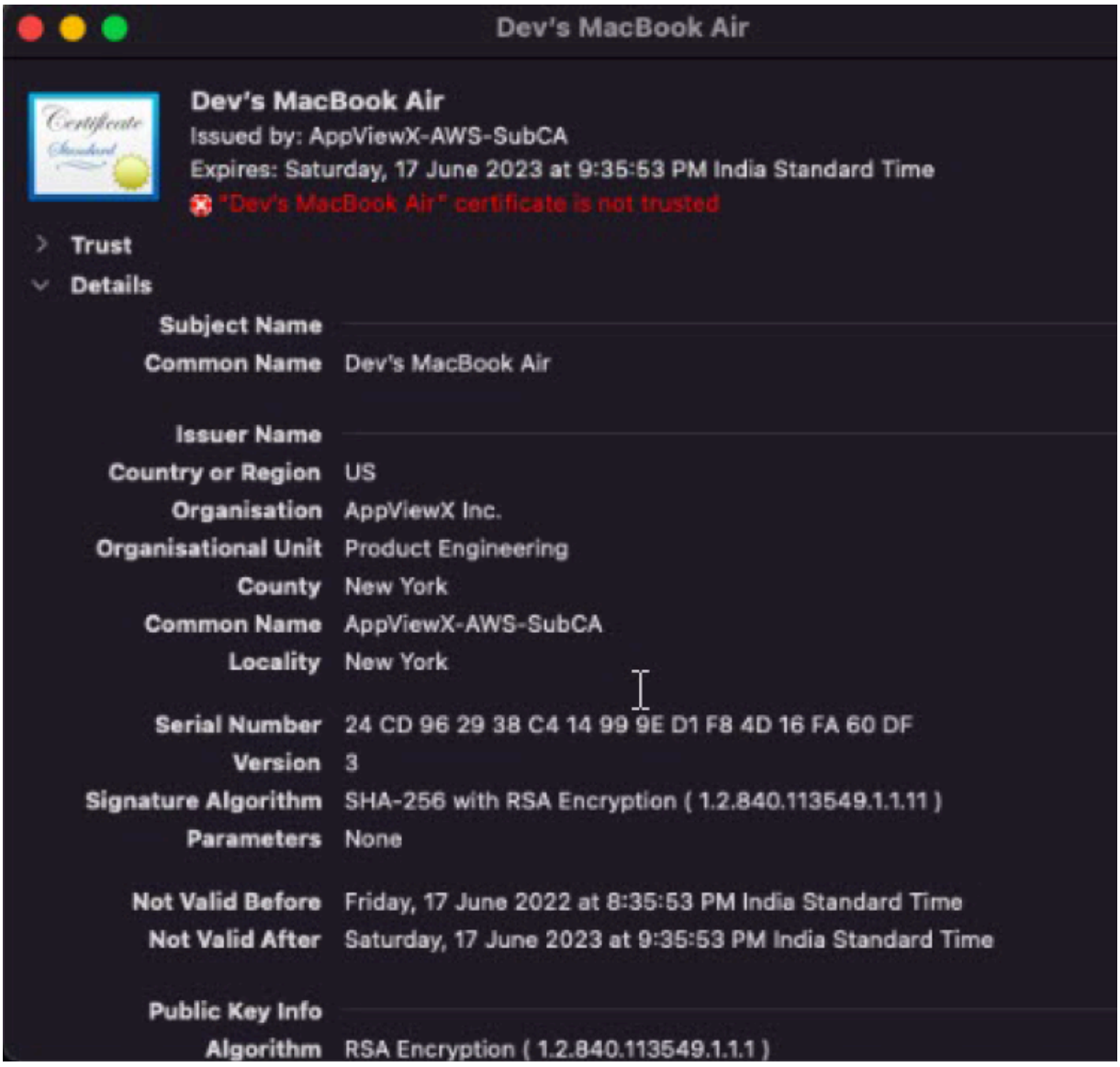
11. To verify the certificate, navigate to **Keychains** (User/System) and validate the certificates that were Installed for each configuration profiles with the respective CN Name.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.



Copyright © 2025 AppViewX, Inc. All Rights Reserved.

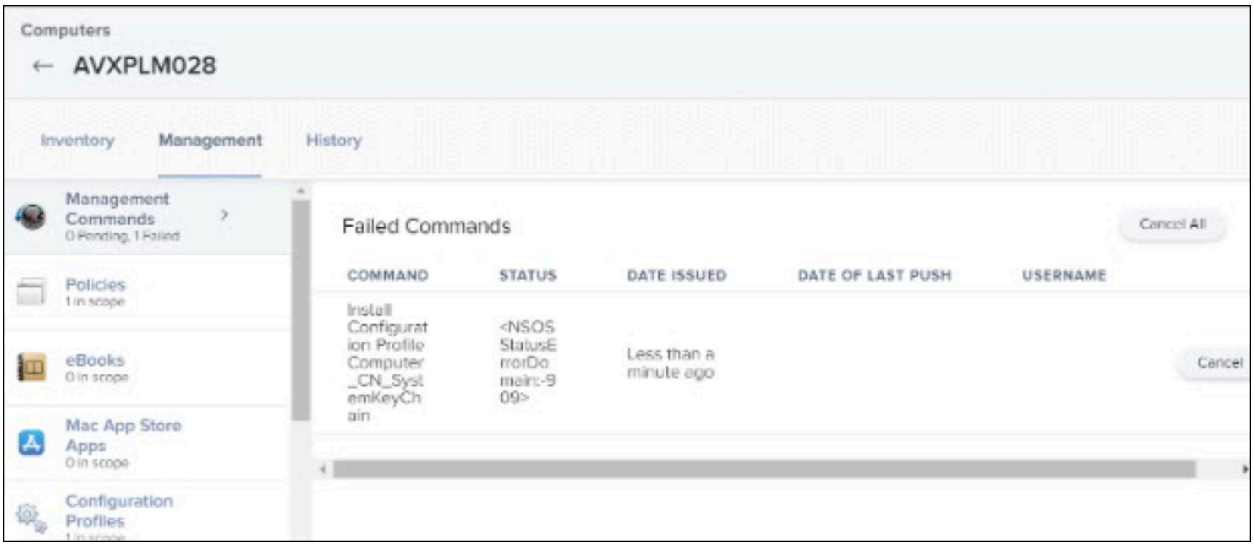




Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Troubleshooting

The failed commands or errors can be viewed here for troubleshooting.



References

#	Topic	URL
1	About Jamf	https://www.electric.ai/blog/jamf-ask-your-it-msp-for-it-by-name
2	Jamf Documentation	https://docs.jamf.com/10.42.0/jamf-pro/documentation/Jamf_Pro_Documentation.html
3	About SCEP	https://www.securew2.com/blog/simple-certificate-enrollment-protocol-scep-explained
4	Mobile Device Configuration Profiles	https://docs.jamf.com/10.30.0/jamf-pro/administrator-guide/Mobile_Device_Configuration_Profiles.html

What's Next?

Refer to the following sections for auto-enrolling protocols:

- AppViewX Integration with Microsoft Intune Integration
- AppViewX Integration with SCEP
- EST Client Configuration Guide
- ACME Configuration Guide - Posh-ACME

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Chapter 7: Glossary

Terms	Definition
ACME	Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating the certificate enrollment to the CA and provisioning the certificate on the requesting entity.
CAA Record	A Certificate Authority Authorization Record specifies which certificate authority is allowed to issue certificate for a domain. If a certificate has CAA record, it means only the CAs listed in the CAA record are allowed to issue a certificate for the domain. If there is no CAA Record, it means any CA can issue certificate for the domain.
Certificate authority (CA)	CA is an entity that verifies the identities of entities such as websites, email addresses, companies, or individuals and links them to cryptographic keys using digital certificates.
Certificate Authority (CA)	A certificate authority or certification authority is an entity that issues digital certificates. It certifies the ownership of the key pair belongs to the subject within the certificate.
Certificate enrollment	This is the process by which a user requests a digital certificate from a Certificate Authority (CA).
Certificate revocation	It is the way in which a certificate is invalidated or revoked before its expiration date. Revoked certificates are listed in the Certificate Revocation List (CRL) maintained by each certificate authority.
Certificate Revocation List (CRL)	Contains a list of digital certificates that have been revoked by the issuing certificate authority before their scheduled expiration date and should no longer be trusted.
Certificate Signing Request (CSR)	It is a message sent to a certificate authority to request a digital identity certificate.
EST	The **Enrollment over Secure Transport** or **EST** is a cryptographic protocol that describes an X. 509 certificate management protocol targeting public key infrastructure (PKI) clients that need to acquire client certificates and associated certificate authority (CA) certificates. **EST** is described in RFC 7030

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Terms	Definition
Heart bleed	**Heartbleed** is a serious vulnerability in the OpenSSL cryptographic library (versions 1.0.1 to 1.0.1f) that allows attackers to access a server's or client's memory, potentially exposing sensitive data such as private keys, passwords, or session cookies. The flaw lies in OpenSSL's implementation of the TLS heartbeat extension, which an attacker can exploit to trick the server into returning chunks of memory that may contain confidential information.
Identity	The digital certificate can also be called a Digital ID or Identity for the subject to whom it is certified.
KMIP	The Key Management Interoperability Protocol is a communication standard protocol that defines message formats for the management of cryptographic keys on a key management server.
MDM	Mobile Device Management (MDM) is the administration of mobile devices, such as smart phones, tablet computers, and laptops.
PKI	A public key infrastructure (PKI) is a technology containing a set of roles, policies, and procedures needed to create, distribute, store and revoke digital certificates and manage public-key encryption.
POODLE	**Padding Oracle on Downgraded Legacy Encryption (POODLE)** is a vulnerability in the outdated SSL 3.0 protocol that allows a man-in-the-middle attacker to decrypt encrypted data, especially in browsers that fallback to SSL 3.0 for compatibility.
Private key	A private key is a secret key that is used to decrypt data and create digital signatures. It must be kept secret and never shared with anyone. The private key is used to authenticate the user and establish a secure connection with the server.
RA (Registration Authority)	It is an entity that verifies the identity of individuals or organizations requesting digital certificates from a CA to ensure only legitimate entities receive them.
ROCA	**Return of Coppersmith's Attack (ROCA)** is a vulnerability in the RSA key generation algorithm that allows an attacker to recover the private key

Copyright © 2025 AppViewX, Inc. All Rights Reserved.

Terms	Definition
	from a public key, potentially compromising systems relying on the affected keys.
SCEP	Simple Certificate Enrollment Protocol (SCEP) is an IETF RFC. This enables network user to request their digital certificate electronically and as simply as possible. Supported by most of the network devices.
SSL/TLS Certificates	SSL refers to Secure Sockets Layer whereas TLS refers to Transport Layer Security. Both are cryptographic protocols providing secure data communication in a network.
URI	**URIs** uniquely identify a resource and can take the form of either a URL or a URN. A **URL** is a resolvable address that specifies where a resource is located on the internet. It typically starts with **http://** or **https://** (for example., https://example.com). URLs are commonly used to identify web services or endpoints in certificates. The same is also applicable for SFTP. A **URN** is a persistent, non-resolvable identifier that names a resource without indicating its location. It typically follows the format urn:<namespace>:<resource> (for example, urn:oid:1.2.3.4). URNs are used in environments where stable identifiers are needed, such as IoT or standards-based systems. To add multiple URIs, separate them with commas. Each entry will be added as a distinct SAN value in the certificate.
X.509 Digital Certificate	X.509 is a standard defining the format of public key certificates. An X.509 certificate is using the widely accepted public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Copyright © 2025 AppViewX, Inc. All Rights Reserved.